MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF INDIVIDUAL PRIVACY; HANDBOOK FOR MUNICIPALITIES AND LOCAL BOARDS

Municipal Freedom of Information and Protection of Individual Privacy

Handbook for Municipalities and Local Boards

Ontario
Management Board of Cabinet

A French-language edition of this publication entitled *Manuel à l'intention des municipalités et des conseils locaux* is available from Publications Ontario at the address below.

On peut se procurer la version française de la présente publication, intitulée *Manuel à l'intention des municipalités et des conseils locaux* à Publications Ontario à l'adresse indiquée ci-dessous.

ISBN 0-7778-0879-X

Copies of this publication are available from:

Publications Ontario
880 Bay Street
Toronto, Ontario
M7A 1N8
(416) 326-5300

February 24, 1993

MEMORANDUM TO: Coordinators of Local Institutions covered by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

FROM: Frank White
Director
Freedom of Information and Privacy Branch
Management Board Secretariat

Enclosed please find the new Handbook for Municipalities and Local Boards. The Handbook has been updated to provide many more practical examples of how the Act may be applied in local institutions. These new examples are possible because of the large number of Orders issued by the Information and Privacy Commissioner since this Manual was first published in 1990. For a more complete examination of the Orders, please refer to the 1993 Annotation also published by this Branch.

You will note that the Manual has changed from a bound edition to one that may be placed in a binder. We hope that this new format will provide advantages such as reducing our costs of printing and distribution for future updates and allowing you easier access to pages for photocopying.

A questionnaire is printed on the reverse side of this page. I encourage you to take time to fill it out and mail it in to us. Your comments help us provide you with better service.

Handbook Evaluation Form

1. Do you like the new format ? Explain.

2. Do you find the new Handbook an improvement on the first edition ? If so, how ?

3. Are there any changes that you would like to see made ?

4. How could the Handbook be more useful to you ?

5. Other suggestions.

Please send this to:

Freedom of Information and Privacy Branch
Management Board Secretariat
56 Wellesley Street West
Toronto, Ontario
M7A 1Z6

or call (416) 327-2187
or fax (416) 327-2190

TABLE OF CONTENTS

FOREWORD

The Municipal Freedom of Information and Protection of Privacy Act came into effect January first 1991.

The purpose of the Handbook is to assist municipalities and local boards to interpret and administer the legislation. The Handbook is intended to serve as a practical guide in carrying out the requirements of the legislation. It should not be used as a substitute for the legislation. Where necessary, the legislation should be consulted. When further information is required on interpretation of the Act, consult the Annotation.

Please address all comments or questions about this handbook to:

Freedom of Information and Privacy Branch
Management Board Scretariat,
56 Wellesley Street West, 18th Floor,
Toronto, Ontario
M7A 1Z6

(416) 327-2187

Copies of the **Handbook for Municipalities and Local Boards** can be purchased from:

Publications Ontario
5th Floor, 880 Bay Street
Toronto, Ontario
M7A 1N8

(416) 326-5300 or 1-800-668-9938

CHAPTER 1

INTRODUCTION TO THE ACT

INTRODUCTION TO THE ACT

Purpose of the Act
[Section 1]

The *Municipal Freedom of Information and Protection of Privacy Act* provides individuals with a right of access to certain records and personal information under the custody or control of institutions covered by the Act.

The purposes of the Act are as follows:

a) to provide a right of access to information under the control of institutions in accordance with the principles that,

- information should be available to the public,
- necessary exemptions from the right of access should be limited and specific,
- decisions on the disclosure of information should be reviewed independently of the institution controlling the information; and

b) to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

Organization of the Act

The Act came into force on January 1, 1991. The Act is divided into four parts:

Part I: Freedom of Information deals with the right of access to records, the exemptions to that right, and access procedures [sections 4-26].

Part II: Protection of Individual Privacy concerns the collection, use and disclosure of personal information. This part also deals with an individual's right of access to his or her own personal information and the right to request correction of that information [sections 27-38].

Part III: Appeal deals with the right to appeal and the procedure involved in appealing a decision made by an institution [sections 39-44].

Part IV: General covers general matters including the charging of fees, offences, regulations and the powers and duties of the Information and Privacy Commissioner [sections 45-55].

The remainder of this introductory chapter will discuss the scope of the Act, definitions of key terms within the Act and the role of the Management Board Secretariat - Freedom of Information and Privacy Branch.

What the Act Covers

The Act covers all municipal corporations, including a metropolitan, district or regional municipality, local boards and commissions. The term institution is defined in section 2 of the Act and is set out in the *Definitions* section immediately below.

This Act applies to any record in the custody or under the control of an institution. This includes records that were created both before and after the Act came into force on January 1, 1991 [subsection 52(1)].

The Act does not impose any limitation on the information otherwise available by law to a party to litigation. Where an institution is required to produce documentary evidence pursuant to rules of court, the exemptions in the Act do not apply [subsection 51(1)]. The Act does not affect the power of a court or tribunal to compel a witness to testify or compel the production of a document. [subsection 51(2)].

Definitions

In this section the following key terms that appear throughout the Act are discussed:

- head
- information and privacy commissioner
- institution
- personal information
- personal information bank
- record
- machine-readable record

Other terms are defined elsewhere in the handbook with its related subject matter. Law enforcement, for instance, is defined under the law enforcement exemption in Chapter 4. The subject index at the end of this handbook provides page references for the terms defined in the text.

Head

The head of an institution is the individual or body made head under section 3. The head is responsible for decisions made under the Act by the institution and for the administration of the Act within the institution. In Chapter 2, a description of the head's responsibilities are discussed in detail.

Information and Privacy Commissioner

The Information and Privacy Commissioner is appointed by the Lieutenant Governor in Council. The Commissioner is an officer of the Legislature and is independent of the government.

The Commissioner hears appeals of decisions made by heads of institutions, issues binding orders, conducts privacy investigations, and has certain powers relating to the protection of personal privacy [section 46]. In Chapter 7, the role of the Commissioner is discussed in more detail.

Institution

Institution is the general term for local organizations, boards and other bodies covered by the Act. An institution is responsible for administering and adhering to the requirements of the Act.

There are three parts to the definition of institution:

1. Municipalities and Their Agencies

   An institution includes a municipal corporation, including a metropolitan, district or regional municipality or the County of Oxford [clause (a) of the definition of institution in section 2].

   Each municipal corporation (villages, towns, townships, cities, counties, and district and regional municipalities) will be a separate institution for the purposes of the Act.

   Each municipal corporation will include as part of the corporation the following bodies: boards of control, sinking fund committees, fence viewing boards, courts of revision, planning advisory committees, property standards committees, cemetery boards, committees of adjustment, land division committees, parking authorities, parks boards, arena boards and recreation boards, and other bodies where all the members or officers are appointed by council.

   For example:

   A board of management for a Business Improvement Area would be covered as part of the municipal corporation because all of the members of the board are appointed by a municipal council.

If *all* of the members or officers of an agency, board, commission, corporation or other body are appointed by [or under the authority of] the council of a municipal corporation, then that body will be part of the municipal corporation for the purposes of the Act. This is the case unless the body is specifically mentioned as a separate institution in clause (b) of the definition (discussed below) or a regulation is passed under clause (c) making the body a separate institution [subsection 2(3)].

Where only *some* of the members of an agency or board are appointed by the municipal institution, that agency or body is not considered part of the municipality for the purposes of the Act.

2. Local Boards

An institution includes a school board, public utilities commission, hydro-electric commission, transit commission, suburban roads commission, public library board, board of health, police services board, conservation authority, district welfare administration board, local services board, planning board, local roads board, police village or joint committee of management or joint board of management established under the Municipal Act [clause (b) of the definition of institution in section 2]. These institutions, some of which are closely connected to municipal corporations, are designated separate institutions for the purposes of the Act.

3. Other Institutions

An institution also includes any agency, board, commission, corporation or other body designated as an institution in the regulations [clause (c) of the definition of institution in section 2].

Sometimes bodies that would normally be part of an institution covered by clause (a) or (b) of the definition of institution may be prescribed as separate institutions for the purposes of the Act.

For example:

> A municipality might have a corporation established under a private statute that operates a convention centre. Except for the fact that the centre is owned by the municipality, it operates as an autonomous entity. In this case it may be appropriate that the centre be designated as a separate institution for the purposes of the Act, for example, The Hamilton Entertainment and Convention Facilities Inc.

Personal Information

Personal information means recorded information about an identifiable individual, including:

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol or other particular assigned to the individual;

(d) the address, telephone number, fingerprints or blood type of the individual;

(e) the personal opinions or views of the individual except if they relate to another individual;

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual; and

(h) the individual's name if it appears with other personal information relating to the individual or where disclosure of the name would reveal other personal information about the individual.

Personal information must be about an identifiable individual, however an individual's name need not be attached to the information to qualify as personal information. A physical description or a photograph of a person attached to other personal information about that person is personal information although no name is ever indicated. This individual is *identifiable* and all personal information relating to the individual must be protected.

Generally, information about a property or a specific municipal address, such as market value assessment, hydro-electric consumption or building permit information, is not personal information. However, records containing such property-related information may also contain an individual's name and personal information such as a home telephone number. Care should be taken to ensure that any disclosure of that personal information complies with the privacy protection provisions of the Act (see Chapter 5 for a discussion of sections 14 and 32 regarding the disclosure of personal information).

An individual's name on its own is not personal information. To be personal information within the meaning of the Act, the name must be associated with other personal information as defined in section 2.

For example:

> An individual's name kept by a social services department would be personal information because the fact that the name was on a record at the department might indicate that the person was, or is, in receipt of public assistance.

An individual, in the context of the Act, does not include sole proprietorships, partnerships, unincorporated associations, corporations, trade unions or law firms or the names of officers of a corporation writing in their official capacity. However, records containing information about these business entities may also contain personal information about individuals and may warrant the protection provided in the Act.

Correspondence submitted to an institution by a representative of a group or association is not the personal information of the author of the correspondence. If the correspondence submitted to an institution is on the letterhead of the organization and signed by an individual in his or her capacity as a spokesperson of the organization, the content of the letter does not qualify as the writer's personal information.

Personal information does not include information about an individual who has been dead for more than thirty years [subsection 2(2)].

The definition of personal information under the Act refers to **recorded** information about an identifiable individual. For the purposes of collecting personal information under Part II of the Act (Protection of Individual Privacy), personal information includes personal information collected orally on behalf of an institution [section 28]. This is discussed in detail in Chapter 5.

Personal Information Bank

A personal information bank is a collection of personal information that is organized and capable of being retrieved using an individual's name or other individual identifier. A collection of personal information in the custody or control of an institution would be a personal information bank if it has the following characteristics:

- it must contain personal information;
- information contained in the bank must be a collection of like or similar information about individuals;
- information must be linked to an identifiable individual; and
- the information must be capable of being retrieved by the individual's name or identifying symbol (such as a number or code name).

For example:

> A public library's circulation records that contain the names, addresses and borrowing records of patrons would be a personal information bank.

Institutions will often have collections of records which contain some personal information, but these would not meet the criteria for the definition of a personal information bank. The Act does not require an institution to rearrange its personal information into personal information banks.

Collections of personal information that meet the characteristics of a personal information bank (as set out above) must be identified and described by the institution. Generally, individuals have the right to obtain information about themselves contained in the personal information banks of an institution. These descriptions must be made available to assist the public in exercising privacy rights.

Record

A record is any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes:

- correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine-readable record, any other documentary material regardless of physical form or characteristics, and any copy thereof; and
- subject to the regulations, any record that is capable of being produced from a machine-readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

The definition of record is very broad and includes virtually every form of information held by an institution. The definition is not restricted to actual physical documents, but includes records that can be created from existing data in a computer bank. Even documents such as computer mail are considered to be records. For further information on computer records, see the definition of machine readable records immediately below.

Handwritten notes or other notations on records form a part of the records. Working copies and drafts of reports and letters are also records.

The Act does not apply to records placed in the archives of an institution by or on behalf of a person or organization other than the institution [subsection 52(2)]. Manuscripts such as diaries and letters donated by a member of the general

public to a municipal archives would not be covered by the Act. However, if an institution places its records in an archives, either its own archives or the archives of another institution, these records are subject to the Act.

Machine Readable Record

In cases where a request is for information that does not currently exist, but is capable of being produced from a machine readable record, the Act gives the requester the right (subject to the regulations) to the information which would answer all or part of a request.

If the process of producing a record from a machine readable format would unreasonably interfere with the operations of an institution, the machine readable record would not be included in the definition of a record as outlined above. Unreasonable interference with operations could include instances where normal business activities would have to stop or change in order to produce the record. It may also include instances where the cost of producing the record would result in the inability of an institution to meet its other obligations.

See R.R.O. 1990, Reg. 823 (the Regulations), section 1 for further information.

Role of Management Board Secretariat

The Freedom of Information and Privacy Branch of the Management Board Secretariat supports the Chair of Management Board of Cabinet as the minister responsible for the provincial and municipal freedom of information and privacy acts. The Branch assists institutions that are covered by the acts by providing training, legal, policy and operational advice. It also drafts legislation and regulations.

The Annotation

The *Annotation* is published by the Freedom of Information and Privacy Branch. The *Annotation* assists in interpreting the provincial and municipal access and privacy legislation. The highlights in the *Annotation* represent the Branch's interpretations of the Orders made by the Information and Privacy Commissioner, Ontario.

Copies of the *Annotation* are available from Publications Ontario, 880 Bay Street, Toronto, Ontario, M7A 1N8 (416) 326-5320.

CHAPTER 2

ADMINISTRATION OF THE ACT

ADMINISTRATION OF THE ACT

Introduction

The *Municipal Freedom of Information and Protection of Privacy Act* sets requirements that must be met by each institution. In many instances, the head of the institution is responsible for fulfilling these requirements. The requirements concern:

- responding to requests for access to records;
- protecting personal privacy;
- providing specific information to the Information and Privacy Commissioner; and
- making information available to the public.

This chapter provides an overview of the administrative responsibilities of the head of an institution, and other issues dealing with the adminstration of the Act.

Head of an Institution

The head of an institution is responsible for decisions made under the Act by the institution and for overseeing the administration of the Act within the institution.

A council or board can designate from among its members an individual or committee to be the head [section 3].

Once the head has been determined the powers or duties of the head can be delegated to an officer or officers of the institution.

Head in Municipal Corporations

Subsection 3(1) of the Act states that the members of a council of a municipal corporation may designate from among themselves an individual or a committee of the council to act as head for the purposes of this Act. This designation must be enacted by by-law. Subsection 3(3) says that if no person is designated as head under this section, the head shall be the council.

This subsection gives a council flexibility in designating who will be the head. The designated head could be an individual, such as the mayor, warden, reeve or councillor, or the head could be a committee of council, such as the executive committee or a special freedom of information and privacy committee. Where an individual is designated, the designation could be to a named individual or to a position, as appropriate.

Careful consideration should be given when deciding who will be designated as the head. The Act requires that decisions about access to information must be made in a relatively short time, usually within 30 calendar days. Because of this, the head will have to be available to make those decisions, unless some or all of the head's duties and powers are delegated. Designating a large committee as the head may present some problems if calling the members together to make decisions about access to information within the 30-day time limit is impractical or difficult.

To revoke a designation, a council would have to revoke the by-law that set out the designation.

Appendix I contains a sample by-law municipalities can adapt to designate the head.

Head in Local Boards and Institutions Other Than a Municipal Corporation

Subsection 3(2) of the Act is similar to that dealing with municipalities in that the members elected or appointed to a board, commission or

other body that is an institution may designate an individual or a committee of the body to act as head of the institution. If there is no designation, the head shall be the members elected or appointed to the board, commission or other body.

The designation, if it occurs, must be in writing.

For example:

> The board of a public utilities commission could pass a resolution in writing designating the chair of the commission as the head of the institution.

To cancel the designation a body should do so in writing.

Appendix II contains a sample written resolution local boards can adapt to designate the head.

Delegation of Head's Authority

Once the council or board has determined the head for the purposes of the Act, the head may choose to delegate some or all of the head's powers and duties under the Act. However, even if the powers or duties are delegated, the head remains accountable for actions taken and decisions made under the Act.

The head may delegate the powers and duties in writing to an officer or officers of the institution or of another institution [subsection 49(1)]. The delegation would usually be to a position, rather than to a named individual. The document that sets out the delegation should make clear the duties and functions being delegated.

The head may also place limitations, restrictions, conditions or requirements on the delegation. A head may wish to delegate only some of the duties and retain certain decision making authority.

For example:

> The head may wish to delegate routine duties such as sending out notices, preparing the annual report, and deciding the fees to be charged, but may retain particularly important duties such as the authority to decide if an exemption from disclosure applies.

Employees who issue notices required by the Act must ensure that they have the delegated authority to do so. Where an employee of an institution denies partial access to records and does not have the written authority to do so, the institution is deemed to have refused complete access to the records at issue. Institutions must adhere to the delegation of authority. Where circumstances change, the institution must revise the delegation of authority.

Appendix III contains some samples of written delegations under the Act, showing all the powers and responsibilities which may be delegated.

It is important to delegate responsibilities to an officer or officers of an institution who, if required, have access to decision makers and who can act quickly within the time periods prescribed in the Act.

Conflict of Interest

A conflict of interest may exist where a public official knows that he or she has a private interest that is sufficiently connected to his or her public duties to influence those public duties. The focus for conflict of interest is frequently financial matters. It may also arise when the head is meeting his or her decision-making responsibilities under the Act.

A head may be in a conflict of interest situation where it is reasonable to assume that he or she is making decisions based on their personal interest rather than the public interest. In some

instances, the conflict of interest may be more apparent than real. It is recommended that delegations of the head's powers reflect the possibility of conflict of interest and provide for alternate decision-makers in those instances.

Responsibilities of the Head

The Act places certain administrative and reporting requirements on heads of institutions. These include:

- meeting time limits and notification requirements;
- considering representations from third parties who may be affected by the disclosure of records;
- making decisions about the disclosure of records and responding to access requests;
- determining the method of disclosing records;
- responding to requests for correction of personal information;
- calculating and collecting fees;
- where necessary, defending decisions made under the Act at an appeal; and
- administering the privacy protection provisions of the Act;

Each of these duties will be discussed in more detail elsewhere in the Handbook. The following administrative requirements are discussed below:

- preparing and making available descriptions of the general types of records and personal information banks maintained by an institution; and
- filing an annual report with the Information and Privacy Commissioner.

Information Available to the Public [Sections 25 and 34]

A head of an institution must prepare and make available descriptions of the institution's records and personal information banks. These descriptions are intended for use by the public to determine the information generally maintained by each institution. Accurate record descriptions enable a requester to submit a more detailed request, thus simplifying the response process.

The records descriptions should be made available in a publicly accessible place or a variety of places such as at the head office of a board, in the clerk's office of a municipality and/or at a public library.

A head must ensure that the descriptions of records and personal information banks are amended as required to ensure that the information is accurate [subsections 25(2) and 34(2)].

The description of records and personal information banks must include:

- a description of the organization and responsibilities of the institution;
- a listing of the general types or classes of records in the custody or control of the institution;
- an index describing all the personal information banks in the custody or control of an institution including:
    - the name and location of the personal information bank;
    - the legal authority for it;

- a description of the types of personal information in the bank;
- how the information is used on a regular basis;
- to whom the personal information is disclosed on a regular basis;
- the categories of individuals about whom personal information is maintained; and
- the policies and practices about the retention and disposal of the personal information;

- the title, address and telephone number of the head; and
- the address to which a request for access to records should be made.

The records descriptions required by the Act need not be complex or lengthy. The descriptions can be prepared in a number of ways and can take advantage of existing material. For instance, municipalities and local boards can use annual reports or promotional brochures that describe how their institution is structured and organized. An institution's file plan can be used to prepare the record list.

Report to Commissioner

Section 26 requires the head to provide an annual report to the Information and Privacy Commissioner. The report must set out:

- the number of requests received by the institution;
- the number of refusals by the head to disclose a record, the provisions of the Act under which disclosure was refused and the number of occasions on which each provision was invoked;
- the number of uses or purposes for which personal information is disclosed if the use or purpose is not included in the statements of uses and purposes set out in the Personal Information Bank Index;
- the amount of fees collected under section 45; and
- any other information indicating an effort by the institution to put into practice the purposes of the Act.

The Commissioner will forward to institutions, the instructions and forms for completing this report. The Information and Privacy Commissioner's Office has developed a computerized tracking system to aid institutions in completing this report. For further information on the computerized tracking system, please contact the Commissioner's office.

Freedom of Information and Privacy Coordinator

Each institution should designate an individual to coordinate freedom of information and privacy activities. This is an important function that assists the institution in meeting the requirements of the Act.

The coordinating responsibilities will vary depending on the size and organization of the institution. Often the function will be a part-time responsibility, assigned to an employee with related duties. The responsibilities of the Coordinator may include staff training, the development of procedures for the administration of the Act, collecting the necessary information for the General Classes of Records and Personal Information Bank indexes and making decisions on requests under the Act (on the delegated authority of the head).

Records Management

Improvement in records management systems throughout municipalities, local boards and commissions is one of the major long term benefits of the Act. The public has a right to expect that each institution knows what records are in its custody or control and where the records are located so that they can be retrieved.

The Information and Privacy Commissioner has stressed the need for institutions to develop and maintain up-to-date retention schedules. Search time would be reduced significantly if an institution could determine if a record has been destroyed by means of a records destruction certificate or other such document. Lengthy searches need not be conducted to determine if a record still exists.

Please see Chapter 3 for further discussion of records management related topics such as custody and control of records, including political and other elected official's records.

Security and Confidentiality of Records

Subsection 47(c) of the Act provides a power to make a regulation setting standards for and requiring administrative, technical and physical safeguards to ensure the security and confidentiality of records and personal information under the control of institutions.

R.R.O. 1990, Reg. 823, section 3 requires measures to prevent unauthorized access to an institution's records and to protect against inadvertent destruction of records. The regulation and guidelines are intended to apply to access and security considerations in the day-to-day administration of an institution's records, rather than access to records in response to requests under the Act.

Accountability

An important first step to establish reasonable measures is to assign responsibility and accountability for the security of the institution's records. This assignment of responsibility and accountability will vary, depending on size and complexity of the institution. Usually, the manager with direct operational responsibility for a program would be assigned responsibility for safeguarding the records generated by that program.

In larger institutions, an internal auditor or other official could co-ordinate security matters throughout the organization and provide technical support to individual managers. Smaller organizations with few staff may wish to assign responsibility for record security to the chief administrative officer or other responsible position.

However an institution assigns responsibility, this assignment should be documented, and appropriate training and awareness should be provided to affected staff.

Determining Security Requirements

Before measures to protect records from unauthorized access can be established, the institution should determine the degree to which access to an institution's records should be controlled. Although it may be necessary to determine appropriate levels of access to individual documents or files, usually this determination would be on the basis of record series. When considering access controls for record series, the level of security should be appropriate for the most sensitive information in the series.

All relevant factors should be taken into account in determining whether access to records should be controlled, and the scope and extent of those controls, including:

- whether or not exemptions are likely to apply to the records;
- the nature of the exemptions (mandatory or discretionary) which may apply;
- the circumstances under which the records were supplied to or created by the institution;
- possible harms which may result from unauthorized access;
- the need to protect the record from tampering; and
- the need to protect unique or original records.

Security Measures

In identifying security measures, the head should balance the cost and complexity of such measures against the possible harms resulting from unauthorized access. Security measures should be appropriate to the nature of the record and to the level of security required.

For paper records, security measures can include:

- clean desk policies, where desks are locked when unattended;
- locking filing cabinets, which are locked when unattended, and where key distribution is limited and documented;
- central file stations, with log-in and log-out procedures for files, accompanied by restriction on the making of copies;
- locked file room with access controlled by file room staff;
- coded file labels, labels using numeric or alpha-numeric codes rather than descriptive texts;
- inclusion of security provisions in contracts with outside suppliers of records storage and disposal services;
- record distribution/circulation policies which limit the production and circulation of records to staff on a need-to-know basis; and
- policies and procedures for using facsimile machines, including policies on types of information which should not be faxed, staff access to and physical placement of the fax machine. Checking procedures such as ensuring that the document is being sent to the correct number prior to sending documents should also be developed. The Office of the Information and Privacy Commissioner has prepared guidelines on the use of facsimile machines which may be consulted.

For computer records, security measures can include:

- positioning terminals in such a manner that passers-by cannot read information displayed on screen;
- password protection for computer hardware, with policies in place governing the assignment, use and deletion of user identifications and passwords;
- encryption of transmitted data or developing guidelines for transmitting confidential information, for example, guidelines for the use of electronic mail;
- tracking systems which monitor the use of data, and which identify system user; and
- inclusion of security provisions in contracts with outside suppliers of information technology services.

The head of an institution shall ensure that only those individuals who need a record for the

performance of their duties shall have access to it. In most cases, the institution would determine which groups of staff need to have access to a particular class or series of records in the performance of duties, and take steps to ensure that access is limited to those groups.

R.R.O. 1990, Reg. 823 also requires an institution to ensure that reasonable measures to protect the records from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

If records are inadvertently destroyed before their proper disposal date, as specified on a retention schedule, requesters are deprived of their right of access under the Act to those records. The head must take all reasonable steps to protect the institution's records from accidental destruction.

In determining what are reasonable steps, the head should consider all relevant factors, including:

- the media of the record (protective measures appropriate for paper records, for instance, may not be appropriate for other media);
- whether copies of the record exist;
- whether the original copy of the record is inherently valuable (such as archival records or signature documents);
- how vital the record is to the functions of the institution;
- the cost of replacing or recreating the record; and
- the cost of available protective measures.

Although measures to protect records from inadvertent destruction will vary among institutions, some common steps which might be considered include:

- making regular back-up copies (disks, photocopies, microfilm), with a copy stored at a site separate from the original or working copy;
- using fire-resistant file cabinets;
- locating record storage/computer operations away from areas where fire or water damage is more likely to occur (for instance away from exposed pipes);
- raising records and records-producing equipment off the floor to prevent flood damage;
- installing smoke detectors and fire-extinguishing equipment (it should be noted that some automatic fire extinguishing systems such as water sprinklers, may themselves pose a hazard to records and computers); and
- ensuring that storage facilities and maintenance practices are appropriate to the record's media (magnetic media, for instance, are especially vulnerable to inadvertent destruction or damage through improper storage). Similarly because magnetic media is often tied to a particular operating system and set of hardware, data stored on that media may not be usable if the operating system or hardware is no longer available.

As with other measures, steps to ensure against inadvertent destruction should be documented by the institution.

CHAPTER 3

ACCESS PROCEDURES

ACCESS PROCEDURES

Introduction

This chapter discusses general information about access, requests under the Act, and how to process requests for access to records. The chapter is divided into the following sections:

Right of Access
Confidentiality Provisions
Existing Information Practices
Copyright Act
Obligations to Disclose
Requests Under the Act
Processing Requests
Locating and Reviewing Records
Granting and Denying Access
Access to Own Personal Information
Checklist of Steps in Processing a Request

Right of Access

Overview

The right of access applies to an existing record, which is defined in chapter 1. There is no obligation to create a record in response to a request under the Act, except in certain circumstances involving information maintained on a computer.

Other points to note regarding the right of access:

- the right of access is not restricted by residency, age or citizenship. An individual need not reside in a particular municipality in order to have a right of access to the records of that municipality, its local boards or commissions;

- the Act is retroactive. It applies to any record that exists regardless of whether or not it was created prior to the Act taking effect on January 1, 1991 [subsection 52(1)]. This subsection also implies that the Act recognizes that although different requirements concerning disclosure of records may have been imposed pursuant to earlier legislation, once the *Municipal Freedom of Information and Protection of Privacy Act* came into force, these records were also subject to the Act; and

- the Act does not apply to records placed in the archives of an institution by private donors other than institutions defined in the Act [subsection 52(2)].

Confidentiality Provisions

Subsection 53(1) provides that the *Municipal Freedom of Information and Protection of Privacy Act* prevails over a confidentiality provision in any other Act unless the other Act or this Act specifically provides otherwise.

The following confidentiality provisions prevail over this Act:

- **Municipal Elections Act, R.S.O. 1990, c.M.53, s.105.**
"No person shall be allowed to inspect the contents of a ballot box in the custody of the clerk except under the order of a judge."

- **Assessment Act, R.S.O. 1990, c.A.31, s.53(1).**
"Every assessment commissioner or assessor or any person in the employ of a municipality or school board who in the course of the person's duties acquires or has access to information furnished by any person under section 10 or 11 that relates in any way to the determination of the value of any real property or the amount of assessment thereof or to the determination of the amount of any business assessment, and who wilfully discloses or permits to be disclosed any such information not required to be entered on the assessment roll to any other person not likewise entitled in the course of

that person's duties to acquire or have access to the information, is guilty of an offence and on conviction is liable to a fine of not more than $2,000, or to imprisonment for a term of not more than six months, or to both."

As a result, on January 1, 1991, all statutory confidentiality provisions ceased to be effective as non-disclosure provisions with the exception of those provisions cited in subsection 53(2) (of MFIPPA) above.

Existing Information Practices

A head may provide information without a formal request under the Act [subsection 50(1)]. The Act is not intended to replace the normal process of providing information. Providing information in response to informal oral or written inquiries will continue. The Act should only be used by the public in cases where information is not available through usual channels. However, when a request is made in writing under the Act, the time limits and procedures in the Act for responding must be followed.

The Act preserves access to information (except personal information) that was available to the public by statute, custom or practice immediately before the Act took effect [subsection 50(2)]. In other words, any information that was available to the public before January 1, 1991 will continue to be available.

For example:

Section 73 of the *Municipal Act* provides that the clerk shall maintain certain official records of the municipal corporation. Section 74 states that the clerk shall provide access to the records specified in section 73 to any member of the public, subject to the *Municipal Freedom of Information and Protection of Privacy Act*. This means that given subsection 50(2) of the Act, pre-existing access continues except in respect of personal information. Therefore, if a record falls under the pre-existing access provision, a formal request under the Act is not necessary.

The same provision exists in legislation establishing regional municipalities, the District Municipality of Muskoka, and the Restructured County of Oxford.

Personal information is excluded from the pre-existing access provision. Disclosure of personal information is governed by sections 14, 32, and 38 of the Act (discussed in Chapters 4 and 5).

Copyright Act

Subsection 27(2)(i) of the federal *Copyright Act* provides that the disclosure of a record pursuant to a provincial freedom of information request is not a violation of copyright. Therefore, this provision means that copies of architects' plans, drawings or specifications may be provided in response to a request under the *Municipal Freedom of Information and Protection of Privacy Act*, unless another exemption applies to the record.

The person to whom the record is provided would still be bound by copyright. When providing access to architects' records, an institution should:

- stamp all plans released under the Act with the phrase "Copyright Act applies to use and reproduction"; and

- ensure that the author is associated by name with the document by including the title block or other indication of authorship on copies of documents released.

Obligations to Disclose

Grave Environmental, Health, or Safety Hazard [Subsection 5(1)]

The Act requires the head to disclose a record that reveals a grave environmental, health, or safety hazard to the public, and where it is in the public interest to do so. In this provision:

- grave means serious, likely to produce great harm or danger;
- public interest includes the interests of the local community in general and not of any particular individual or group of individuals; and
- the information must be in record form.

If these conditions are met, the record must be disclosed as soon as possible. There is no requirement that a request under the Act be made before the head is required to act.

For example:

> Where the head possesses records indicating that a beach is unsafe because of high levels of pollution, he or she is obliged to alert the public to the danger.

Before disclosing a record, the head must give notice to any person to whom information in the record relates if it is reasonable to do so in the circumstances [subsection 5(2)]. The notice need not be in writing. Due to the urgency of the circumstances contemplated, the head is not required to wait for any prescribed period before disclosing the record or obtaining any representations.

This section applies despite any other provision of the Act.

Compelling Public Interest [Section 16]

Where certain exemptions apply to a record, disclosure may be required if a compelling public interest in the disclosure of the records clearly outweighs the purpose of the exemption. This provision applies to the following exemptions:

- Advice or recommendations [section 7];
- Relations with governments [section 9];
- Third party information [section 10];
- Economic and other interests [section 11];
- Danger to safety of health [section 13]; and
- Personal privacy [section 14].

This section does not apply to exemptions dealing with records of closed meetings [section 6], law enforcement [section 8], solicitor-client privilege [section 12], or published information [section 15].

The interest in disclosure must be compelling, i.e. strong or overwhelming. The public interest must also clearly outweigh the purpose of the exemption. There is a balancing required by weighing the public interest against the purpose of the exemption. The results of that balancing test must be clear and definitive.

Both the head of the institution and the Information and Privacy Commissioner can determine if the compelling public interest provision applies to the disclosure of a record.

Requests Under the Act

What is a Request?

Under the Act, a request for access to records must be made in writing and must provide sufficient detail to enable an experienced employee of the institution to identify the record(s) requested [subsection 17(1)].

If an individual is seeking access to his or her own personal information, the request must also identify the personal information bank or the location of the personal information being requested [subsection 37(1)]. If, after a thorough search, the institution cannot locate the requested personal information and the requester cannot provide any credible evidence to support the existence of records, the records are deemed not to exist in a personal information bank.

Sometimes a request might be in the form of a question. For example, a requester might write, "Does the municipality have any information about child care services?" In this situation it is unlikely that the institution could determine what information the requester wants. For this reason, requests in the form of questions are not generally acceptable and should be clarified with the requester before proceeding to process the request.

There is a prescribed form for access requests, however a letter that makes reference to the Act would be considered a request. If an institution is in doubt about whether or not it should treat a letter as a request under the Act, the requester should be contacted to seek clarification.

A request for access to hardcopy records must be for records that exist at the time a request is received. There is no requirement to compile information from a number of records to create a new hardcopy record in response to a request.

For example:

> A requester might ask to see a copy of an audit report of a planning board. It might be that an audit report was never prepared by the planning board. If this is the case the planning board would not be obliged to prepare one to satisfy the request.

A municipality might get a request for access to a record that was destroyed according to the municipality's records retention by-law. In response to a request for the record, the municipality would advise the requester that the record does not exist.

A request may also be made for access to records that are capable of being produced from a machine-readable record using the hardware, software and technical expertise normally used by the institution.

For example:

> An institution may generate a report in a certain format from data in a computer file. A requester under the Act may ask for a different kind of report using the same computer data sorted or presented differently. Requests for machine readable records are subject to R.R.O. 1990, Reg. 823, section 1.

Where the information requested is personal information, the computer record must be made available in comprehensible form [subsection 37(3)], i.e., a record which merely shows computer codes rather than information intelligible to the requester would not be in comprehensible form.

Translating Requests

The Act does not require that records be translated into the language of the requester. Some municipalities and local boards offer services in a number of different languages. When responding to requests, institutions should follow the policies and practices set by their respective councils and boards.

Clarifying Requests

An institution is under an obligation to assist the requester to clarify the request where the request does not sufficiently describe the record sought. Clarifying a request is helpful to both the institution and the requester. After a request

has been clarified it should be clear to each party what records are being requested [subsection 17(2)].

For example:

> A requester might ask to see "all the minutes that the Hydro-Electric Commission has". Does this mean all the board minutes, the committee minutes, or both? For what year?

In the example above, it might be that the requester was interested in only the board minutes from a particular date or date range. By clarifying the request the institution could save considerable time searching through records and preparing them for release. It would also save a requester considerable costs if a fee is charged.

The records descriptions and descriptions of personal information banks can be used to help clarify requests. (See Chapter 2 for a discussion of record and personal information bank descriptions.)

Appendix IV contains a sample letter that can be sent to a requester when a request needs to be clarified.

Who Can Make a Request?

Any person can make a request for access to records. In this instance a person includes individuals and organizations such as corporations, partnerships and sole proprietorships. The right of access is not limited by citizenship or place of residence.

There may be situations where one person represents another individual. The Act provides that any right or power conferred on an individual by the Act may be exercised by:

- the personal representative of a deceased individual only if the exercise of the right or power relates to the administration of the individual's estate. The personal representative would be the executor named in a will or if there is no will, the administrator appointed by a court [subsection 54(a)];

- a committee for a person if one has been appointed or the Public Trustee. A committee can be appointed by a court for an individual who is incapable of managing his or her own affairs. The Public Trustee may become an individual's committee under the *Mental Health Act* or the *Developmental Services Act* [subsection 54(b)];

- the person having lawful custody of a child under the age of sixteen [subsection 54(c)]; or

- a person with the written consent of the individual.

The rights and powers which an individual may exercise include the right to make access requests, the right to consent to the collection, use and disclosure of personal information and the right to request correction of personal information.

Processing Requests

A records management system that includes a filing system and storage, retrieval and records retention procedures will help an institution process requests for access to information.

Time Limits

In general, requests for access to records must be dealt with within 30 calendar days from the date a complete request is received [section 19]. A complete request is one which has been clarified or one which provides sufficient detail to allow the institution to understand what information is being requested. The 30-day time period does not start to run until the day after the institution receives a complete request. If a time limit under the Act expires on a Sunday or statutory holiday the time limit is extended to

FIGURE 1

Processing a Request

1. RECEIPT OF REQUEST

- Written access request received [17(1)]
- Sufficient detail? [s.17(1)]
- Institution to assist in reformulating request? [s.17(2)]
- Date stamp request, open file, begin tracking

2. LOCATE RECORD

- Does record exist? [s.17(1)
- If machine readable record, can record be produced? [s.2]
- Does institution have custody or control/greater interest in record? [s.18(2)(3)]
- Transfer request if necessary [s.18(2)(3)]

3. PRELIMINARY REVIEW

- Potential exemption? [s.6-15]
- Third party notices and representations required? [s.21]
- Extension (and notice) required? [s.20]
- Fee estimate over $25.00? [s.45(3)]
- Deposit required?
- Suspend 30-day count?

4. PROCESS REQUEST

- Retrieve records
- Do exemptions apply?
- Compelling public interest? [s.16]
- Determine access method (original vs. copy) [s.23]
- Sever records where required [s.4(2)]
- Determine fee [s.45]
- Fee to be waived? [s.45(4)]

5. GRANT/DENY ACCESS

- Provide notice *re* access, exemptions and fee [s.19,22(3)]
- Where appropriate, provide third party notice and wait 30 days
- Collect fee where applicable

6. END

- Provide record or part of record to requester

or

- Provide notice that access is denied or record does not exist [s.22(1)]
- Document request
- Close file

the next day which is not a Sunday or statutory holiday.

Where an institution receives a broad request which is subsequently narrowed by the requester, the 30-day time period begins on the date the original broad request was received. Where the original broad request provided the institution with sufficient detail regarding the nature of the records being requested, the request is deemed to be merely narrowed, not clarified.

For example:

> An individual requests the results of a police investigation, including all correspondence between the police agency and an outside organization relating to a specific case. The requester later limits his request to one specific report regarding the case. This request would be considered narrowed and not clarified. The original request contained sufficient detail for a staff person to identify the records. In this case, the 30-day time limit would begin on the day the first (broad) request was received.

The time limit for responding to a request is automatically extended where notice is given to a third party under section 21.

Institutions that wish to courier materials to requesters and third parties should note that courier companies cannot deliver to a post office box. A street address is required.

Receipt of Request and Opening Request File

The first step an institution should take when a request is received is to stamp the date on the request. This is important because of the time limits in the Act. Requests arriving at an institution should be routed quickly to the person responsible for handling freedom of information and privacy matters to ensure that time is not wasted while the request works its way through the institution to the appropriate person(s). A notice should be sent to the requester acknowledging receipt of the request.

Once the person responsible for dealing with access requests receives the request, a file should be opened. The file cover can be printed with information that will help route the file if it must be sent to other divisions of the institution. If return dates are filled in on the folder this will help keep people aware of the time deadlines. The file folder can also serve as a record of the decisions taken with respect to the file. To help track requests for access to records it is a good idea to have a different coloured folder for freedom of information and privacy matters.

A tracking and recording form is useful to record the actions taken to process a request. It allows the institution to know at a glance how a request was processed and what decisions were made with respect to the file. Also, by keeping a recording and tracking form, it is evident what has to be done to complete the file.

Do You Have the Record?

The Act applies only to records in the custody or control of an institution covered by the Act.

In determining whether it has custody or control or a record, an institution must consider all aspects of the creation, maintenance and use of a particular record.

Custody of a record includes the keeping, care, watch, preservation or security of the record. While physical possession of a record may not always constitute custody, it is the best evidence of custody.

Control of a record means the power or authority to make a decision about the use or disclosure of the record.

For example:

Records of the public works department of a municipality would be both in the custody and under control of the municipality.

Political records belonging to a municipal councillor or elected official of a board or commission may come within the custody and control of an institution if these records are integrated with other files held by the institution. When no steps are taken to separate the maintenance and storage of political records from municipal records and an employee of the institution has responsibility for their care, these records would then be subject to the Act.

In addition, where a record in the custody and control of an elected official is communicated to an officer or employee of an institution, the record may now be considered to be in the custody and control of the institution.

In the examples above, the Act might apply to the records because the institution would have either custody or control of the records (or both).

The following questions can be used to determine custody or control. This is not an exhaustive list of possible considerations:

- was the record created by an officer or employee of the institution?
- what was the intended use of the record?
- does the institution have possession of the record either because it has been voluntarily provided by the creator or pursuant to a mandatory statutory or employment requirement?
- if the institution does not have possession of the record, is it being held by an officer or employee of the institution for the purpose of his or her duties as an officer or employee?
- does the institution have a right to possession of the record?
- does the content of the record relate to the institution's mandate and functions?
- does the institution have the authority to regulate the use of the record?
- to what extent has the record been relied upon by the institution?
- how closely is the record integrated with other records of the institution?
- does the institution have the authority to dispose of the record?

If an institution has custody or control of the records and will be responding to a request for access to records, it would proceed to gather and review the records to determine what will, or will not, be released.

Forwarding Requests

Institutions may receive requests that would be more properly handled by another institution. Depending upon the circumstances, the institution will either forward or transfer the request to the second institution. Forwarding and transferring requests are discussed below.

If an institution does not have the record(s) that were requested in its custody or control, the institution must make reasonable inquiries to determine if another institution has the record(s) [section 18]. What would be reasonable inquiries depends on the circumstances.

For example:

A regional municipality might receive a request for information about a program run

by a local municipality in the region. If the region knows that the matter is a local responsibility it would be reasonable to expect that the region would contact the local municipality to see if it is appropriate to forward the request to that local municipality.

Under the Act a request can also be forwarded to an institution covered by the (provincial) *Freedom of Information and Protection of Privacy Act* and vice versa. Institutions covered by that Act include provincial government ministries, agencies, boards, corporations and commissions, community colleges and district health councils.

To assist institutions in determining where to forward or transfer a request, the provincial government has published a *Directory of Institutions* that lists the institutions covered by both the municipal and provincial freedom of information and privacy acts.

If a local institution does not know where to forward a request, it should inform the requester of this and indicate what steps were taken to make the inquiries.

If the head determines that another institution has custody or control of the record(s), the request must be forwarded within 15 days of the date the request was received. The institution must also notify the requester that the request has been forwarded to another institution [subsection 18(2)(b)]. (See Appendix IV for a sample notification letter.)

Transferring Requests

In some cases more than one institution will have copies of the requested record(s). An institution (including those under the provincial Act) might determine that another institution has a greater interest in the record. In that case the request may be transferred to the second institution [section 18]. An institution is under no obligation to transfer the request, but may do so if it wishes.

Another institution has a greater interest in the record if:

- the record was originally produced in or for another institution; or
- if the record was not originally produced in or for another institution, the other institution was the first institution to receive the record or a copy of it.

For example:

> Both a municipality and provincial government ministry might have a copy of an environmental impact study that was originally prepared for the provincial government. In such a case the municipality might decide to transfer the request to the provincial ministry.

If an institution is in doubt about whether or not the second institution that created a record might apply an exemption from disclosure to the record, the first institution might consider transferring the request to the second institution.

If it is appropriate to forward or transfer a request it is important to act quickly. The 30-day time limit begins when the request is received at the first institution and continues to run before it is forwarded or transferred to the second institution. Due to time constraints, institutions transferring or forwarding a request should immediately telephone the Freedom of Information Coordinator at the second institution. This will give the second institution more time to locate records that are responsive to the request.

The second institution that receives the request has the remainder of the 30-day period to respond [subsection 18(5)]. The time for responding does not stop running while the

request is in transit, however, the second institution may send a notice to an affected third party, require a time extension, or issue a fee estimate, all of which would change the original deadline. An institution should choose a fast and reliable method of forwarding or transferring a request.

An institution cannot forward or transfer a request to a federal department. The requester must be instructed to re-submit the request under the [federal] *Access to Information Act* or the *Privacy Act*.

For example:

> All records of indictable criminal convictions, supported by fingerprints are held by the RCMP. While Provincial and Municipal police agencies have access to Criminal History information, an individual requiring an official copy of their own history must be directed to submit such a request to the RCMP, supported by their fingerprints. If the request was made to a Municipal or Provincial police agency, it cannot transfer such a request. The request must be re-submitted to the federal department (the RCMP).

An institution must notify a requester if it forwards or transfers a request to another institution [subsection 18(3)]. (See Appendix IV for a sample notification letter.)

An institution which has forwarded or transferred a request should retain documentation of its actions prior to the forwarding or transfer.

Locating and Reviewing Records

Once an institution determines that it is the appropriate institution to respond to a request, the institution must search for the requested records, examine them and decide what will be released. During the review of the records, an institution may find it necessary to extend the time period to respond to a request, notify affected parties and/or issue a fee estimate. In these instances the time period for processing the request is suspended or extended.

Search for Records

Searches for records responsive to a request should include, where practicable, enquiries of staff responsible for the issue(s) the records concern at the time the records were created or might have been created. Enquiries should also be made for any briefing materials relevant to the issue.

The following should also be considered when searching for records:

- identify the specific files and data banks that should be searched by the institution in response to the request;
- determine whether records and/or types of records the requester claims should exist within the institution's files, are contained in the files that the institution did search; and
- identify and assess whether other files and data banks might contain records responsive to a request.

Steps taken by an institution to locate a record could be verified by affidavit evidence and by other evidence in the form of memoranda prepared by persons who conducted the searches.

Time Extensions

A head can extend the 30-day time limit for responding to requests for a period that is "reasonable" in the circumstances [section 20], if one of two conditions exists:

- the request is for a large number of records or necessitates a search through a large number of records and meeting the time

limit would unreasonably interfere with the operations of the institution; or

- consultations with persons outside the institution are necessary to comply with the request and cannot be completed within the time limit.

Under the first condition for extending time, interference with the operations of the institution must relate to a request for a large number of records or require an extensive search through a large number of records.

Under the second condition for extending time, an institution may need to consult with persons outside the institution about the records.

For example:

> A municipality might have to consult with the provincial government to determine if the exemption from disclosing records under section 9 (relations with governments) applies to the requested records.

The 30-day time limit can only be extended once.

An institution cannot combine numerous requests and deal with them en bloc rather than individually as requested and then request a time extension because a search through numerous records or consultation is necessary.

The Act provides institutions with a clear and relatively short time limit for responding to requests. The time limit can be extended only in the circumstances set out in section 20. The head must determine whether *any particular request* involves a large number of records or consultations that cannot reasonably be completed within the 30-day time limit.

There are two legitimate courses of action that an institution might consider when compliance with the time limit set out in the Act places an excessive strain on resources. They are as follows:

- negotiate with the requester who sends in numerous requests as to whether he or she would consent to waive the 30-day limit for each of the requests in favour of a response within 30 days in respect of certain *priority* requests and a longer response time in respect of others.

- if at all possible, allocate the institution's resources in such a way that it can import, on an emergency basis, additional staff to assist those routinely working on freedom of information requests in situations in which there is a sudden influx of requests.

The institution's Freedom of Information Coordinator could work on a one-to-one basis with the requester to work out a compromise. Where possible, the coordinator may offer the requester access to the originals, a few at a time, and the requester could then determine which records he or she would like copied.

An institution should consider each request separately and decide on a case-by-case basis, whether a request's volume justifies a section 20 extension.

If the head extends the time limit, the head must give the requester a written notice [subsection 20(2)] that sets out:

- the length of the extension;

- the reason for the extension; and

- the fact that the requester can ask the Information and Privacy Commissioner to review the decision to extend the time period.

Appendix IV contains a sample notice of time extension.

Notices to Affected Third Parties

Periodically, records will contain information that concerns a person other than the requester. In this instance, a person may be another individual or a corporation, partnership or other legal entity considered to be a person. Before granting access to a record that affects a third party, a head must give written notice to third parties to whom the information relates. The information is considered to affect a third party if:

- the head has reason to believe that the record contains third party information referred to in subsection 10(1); or

- the record contains personal information that the head has reason to believe might, if released, constitute an unjustified invasion of personal privacy [subsection 14(1)(f)]. (See Chapter 4, Exemptions)

A notice to an affected party gives the affected party an opportunity to make representations about the proposed disclosure of records that affect them.

If the head intends to release the records, then the head will give the affected party a notice [subsection 21(2)]. The notice must contain:

- a statement that the head intends to disclose a record or part of a record that may affect the interests of the person;

- a description of the contents of the record or the part that relates to the third party; and

- a statement that the person may, within 20 days after the notice is given, make representations to the head as to why the record or part of the record should not be released.

The notice must be given within the initial 30-day period after a complete request is received or, if there has been an extension of time under subsection 20(1), within that extended time period.

The third party has 20 days after the notice is given to make representations to the head [subsection 21(5)]. Representations are to be in writing unless the head permits them to be made orally. After the representations are made (or after the 20-day period for representations has elapsed), the head must decide within 10 days whether or not to disclose the record.

If affected third parties have been notified, this will delay the processing of a request. Therefore, the head must notify the requester of the delay [subsection 21(4)]. It is advisable to do this at the same time that the affected third party is notified. The notice to the requester must state:

- that the disclosure of the record or part may affect the interests of a third party;

- that the third party has an opportunity to make representations concerning the disclosure; and

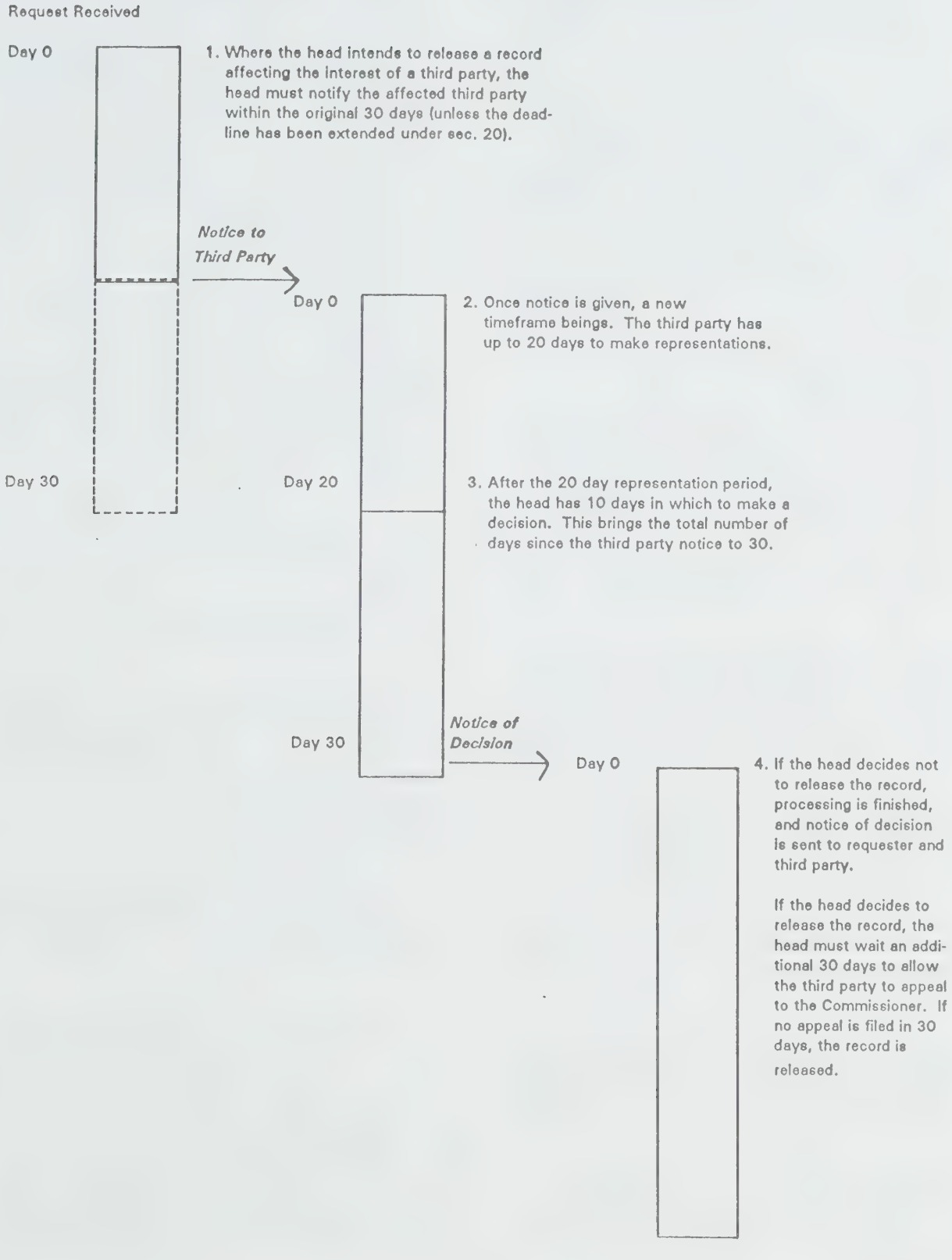
- that the head will decide within 30 days if the record or part will be released.

Appendix IV contains sample notification letters to third parties and to requesters.

Fee Estimates/Interim Notices

In processing a request, it may become clear that fees will be involved. If it appears that the costs of processing the request will be over $25.00, the requester must be given a fee estimate before the head gives access to the records [subsection 45(3)]. Section 19, however, requires the head to notify the requester within 30 days of his or her decision regarding access to the requested records.

FIGURE II
Third Party Notice and Representation Process
Section 21



Therefore, both the fee estimate notice and a notice of decision on access must be issued within the 30-day period (unless there has been a time extension or a third party notice issued). This can be handled in two ways:

- where the number of records is not large or unduly expensive to retrieve, it will be a relatively straightforward matter for the institution to review the records and provide the requester with both a detailed fee estimate and a section 19 decision about the disclosure within the 30-day period. In this case, the fee estimate amounts to the same as a final fee statement, and no records would be severed, copied, or released until the fee is paid or waived.

- there may be cases where it would be unduly expensive for an institution to gather and review the records to make a decision before a fee estimate is agreed to and a deposit paid. There may be, for instance, requests involving large volumes of records or records housed in a variety of locations.

In such a case, the head provides the requester with a notice containing an interim decision about access under section 19 and a fee estimate under subsection 45(3). The decision on access is an interim decision because the head will not yet be in a position to fully determine whether and how exemptions will apply. Both the interim decision and the fee estimate are based on one of the following methods:

- consulting with an employee of the institution who is familiar with the type and contents of the records; or

- basing the interim decision and fee estimate on a representative (as opposed to haphazard) sampling of the records.

The interim decision lets the requester know that certain exemptions may apply to the records. Since this is not a final decision, it is not binding on the institution and is not subject to appeal. However, the fee estimate may be appealed [subsection 45(5)].

The time period for responding to a request is suspended after the notice containing the interim decision and fee estimate is issued. The time begins to run again once the institution receives a deposit from the requester or the head grants a fee waiver, or the issue of fees has been resolved after an appeal to the Information and Privacy Commissioner.

In all cases, the fee estimate should be based on an examination of the records and should provide the requester with as much information as possible about the costs that will be incurred in processing the request. The estimate should also indicate that the requester may ask for a fee waiver.

See Chapter 6 for information about chargeable costs, the calculation of fees, deposits and fee waivers.

Granting and Denying Access

Once a head has made a decision about access, the head must give written notice of the decision to the requester and any affected third parties. The notice must be given within the 30-day time period (or within the period of extended time, if any).

However, if third party notices have been given, the notice of a decision concerning disclosure cannot be given until:

- a response from a third party has been received; or

- after the 20-day period in which a third party can respond to a third party notice has elapsed [subsection 21(7)].

If a head does not give the requester notice of his or her decision within the 30 days (or within

the timeframes extended under section 20, extension of time, or subsection 21(7), third party notice procedure) the head is deemed to have refused access to the record. The requester may then appeal to the Information and Privacy Commissioner/Ontario.

Methods of Severing Records

If part of a record that has been requested falls within one of the exemptions and other information in the record can be disclosed, the head must disclose as much of the record that can be reasonably severed without disclosing the exempt material [subsection 4(2)].

To sever records an institution can blank out the exempt material on a photocopy of the record and release a copy of the photocopy to the requester. In some cases an institution can use removable tape over the exempt parts of a record and make a photocopy for release.

Whenever an institution severs records, copies of the severed records should be kept on file by the institution as a record of what parts of records were released.

Granting Access to Records Where There is an Affected Third Party

If a head decides under subsection 21(7) to release a record in whole or in part that affects a third party and has heard representations from the third party or the time period for making representations has expired, the head must notify the requester and the affected third party that:

- the person to whom the information relates may appeal the decision to the Commissioner within 30 days; and
- the requester will be given access to the record or part unless an appeal is filed within the 30 days after the notice is given [subsection 21(8)].

The notice should be very clear that the requester will be given access to the record or part unless the affected third party appeals to the Commissioner within the 30-day time limit.

Making the Record Available

A requester who is granted access to a record or part of a record is given a copy, unless it would not be reasonable to reproduce the record or part because of its length or nature. In these cases the person must be given an opportunity to examine the original record or part.

For example:

> A municipality might have a collection of hand-coloured maps kept under strictly controlled conditions. Because of the nature and condition of the maps, it might be more reasonable to give the requester an opportunity to examine the maps rather than reproduce them.

Access to Original and Copying

Sometimes a requester may ask to examine the original record or part rather than have a copy. The head shall allow the requester to examine the record or part, if it is feasible to give the requester that opportunity [section 23].

Once the requester has examined the original record or part and wants parts of it copied, the requester must be given a copy of what is wanted, unless it would not be reasonable to reproduce the record or part because of its length or nature.

If access to the original record would compromise the security of the record, it may not be reasonable to provide access to the original.

For example:

> A municipal archives might have genealogical records in the original form and on microfiche. Given the age and condition of the original documents, it might not be practicable to give access to them.

If a photocopy is made of the original severed record, the requester is charged for the cost of photocopying.

Granting Access to Records in Their Entirety

If a record is to be released in its entirety, a requester is informed of the decision to grant access [subsection 19(1)]. Appendix IV provides an example of a notification letter.

If the institution is granting access to records to an individual who has requested his or her own personal information, the institution must confirm the identity of the individual to ensure that the personal information is disclosed only to the individual to whom it relates or to that individual's representative. Further information about verifying an individual's identity is discussed later in this chapter.

Denying Access to Records or Parts of Records

If a head has decided that the records or part of the records fall within an exemption, a head must refuse to disclose the information if the records or parts are subject to a mandatory exemption. A head may refuse to disclose them if they fall within a discretionary exemption, but does have the option of releasing the records. A notice of refusal [section 22] must state:

- if the record does not exist, that the record does not exist and the requester may appeal the question of whether or not the record exists to the Information and Privacy Commissioner; or
- if the record exists,
  - the specific provision of the Act under which access is refused;
  - the reason the provision applies to the record;
  - the name and position of the person responsible for making the decision; and
  - that the requester can appeal the decision to the Information and Privacy Commissioner.

An institution must describe the withheld record(s) sufficiently to allow a requester to make a reasonably informed decision whether or not to appeal. This should include a detailed description of the withheld record(s) or an index. Care should be taken not to disclose any names when describing the withheld record(s).

Appendix IV contains a sample notice denying access to records.

Refusing to Confirm or Deny the Existence of a Record

In certain circumstances when an institution has decided to refuse access to records, it may also refuse to confirm or deny the existence of a record, if the record relates to law enforcement [subsection 8(3)], or if disclosure of the records would constitute an unjustified invasion of personal privacy [subsection 14(5)].

The notice of refusal [subsection 22(2)] to the requester must state:

- that the head refuses to confirm or deny the existence of the record;
- the provision of the Act (either subsection 8(3) (law enforcement) or subsection 14(5) (unjustified invasion of personal privacy)) on which the refusal is based;

- the name and office of the person responsible for making the decision; and

- that the requester may appeal the decision to the Information and Privacy Commissioner.

There may be instances where acknowledging that a record exists could hamper law enforcement matters or invade an individual's privacy.

For example:

> A social services department that acknowledges that a record about a particular individual exists may invade that individual's personal privacy because the acknowledgement would be a strong indication that the person was, or is, in receipt of social assistance.
>
> A police agency that acknowledges that a record exists about a particular individual may compromise an investigation before a decision is made to lay a charge.

Access to Own Personal Information [Subsections 36(1) and 37(1)]

The *Municipal Freedom of Information and Protection of Privacy Act* provides an individual with a right of access to his or her own personal information, whether or not the information is held in a personal information bank.

A request must be in writing and must identify the personal information bank where the record is held or the location of the personal information. The personal information bank index will assist the requester in locating the specific personal information bank that contains his or her information.

Identification Required for Access

When releasing personal information upon request, an institution must verify the requester's identity and ensure that the records are safely transmitted. It is up to the institution, on a case-by-case basis, to satisfy itself as to a requester's identity before releasing personal information to the individual. This can be done by various means, for example:

- ask for photo identification, i.e. driver's license or a passport;

- spelling of names, address, telephone number, signature, handwriting, etc., should be reviewed and compared with the information that an institution may have on file. Any discrepancies should trigger further inquiry; or

- question the requester on unique personal information contained in the record itself. For example, a Health Unit may ask for an Ontario Health Card number.

Personal attendance should not be the standard form of verification used by an institution as many individuals do not posses photo ID.

In cases where an institution is highly suspicious of the requester's identity, an institution must take whatever reasonable steps it believes will satisfy itself as to the identity of the requester.

Comprehensible Form

Personal information must be provided to the individual in a comprehensible form and in a manner which indicates the general terms and conditions under which the information is stored and used [subsection 37(3)].

Personal information may be stored in such a manner that it would not be readily understood by the individual. For instance, information

produced in coded form is meaningless without providing the key to the code. Information provided in response to a request under the Act should be decoded, or the code or key provided, so the information can be understood by the individual.

Correction of Personal Information [Subsection 36(2)]

Every individual who is given access to his or her own personal information has the right to request correction of the personal information if he or she believes that the information contains errors or omissions [subsection 36(2)].

The right of correction applies only to personal information to which an individual is given access. The meaning of the word *correction* incorporates three elements:

- the information at issue must be personal information; and
- the information must be inexact, incomplete or ambiguous; and
- the correction cannot be substitution of opinion.

If the correction sought is merely a substitution of opinion, then it will not qualify as a correction to personal information. A statement of disagreement may be attached. The Access/Correction Request form may serve as a statement of disagreement.

Once a head has been asked to correct personal information, the head must consider whether or not the information submitted for correction can be verified. In some cases, documentary proof should be requested, especially if the information impacts on an individual's financial status or eligibility for a benefit.

If a requested correction of personal information is not made, the individual should be informed of the reasons the correction was not made and that the individual has the right to:

- appeal the decision to the Information and Privacy Commissioner;
- require that a statement of disagreement be attached to the information; or
- have any person or body to whom the personal information was disclosed within the last twelve months notified of the correction or statement of disagreement [subsection 36(2)].

The Act does not specify the time period within which a response must be provided to a request for correction. The general 30-day period is considered reasonable.

Checklist for Processing a Request

A Request is Received

1. Is the request in writing? [subsection 17(1)]
2. Does it provide sufficient detail to enable you to identify the requested record(s)?

   If not, assist the requester to rewrite the request [subsection 17(2)].
3. Date-stamp the request, open a file and prepare a tracking and recording form.

Do the Requested Records Exist?

1. Do the records exist or are they capable of being reproduced from a machine-readable record?

   If not, notify the requester that the records do not exist [subsection 22(1)(a)].
2. Does your institution have custody or control of the records?

If not, make reasonable inquiries to determine where to forward the request, and forward the request within 15 days of receipt. Notify the requester if the request is forwarded [subsection 18(2)].

If you do not know where to forward the request, notify the requester that the records do not exist and that the requester can appeal to the Information and Privacy Commissioner [subsection 22(1)].

3. If your institution and another institution have copies of the records, determine which institution has a greater interest in the record and if appropriate, transfer the request to the other institution within 15 days of receiving the request. Notify the requester of the transfer. [subsection 18(3) and (4)].

Locating and Reviewing the Records

1. Gather the records or a sample of the records and review them.

2. Will some of the exemptions apply?

3. Do you need more time to process the request?

4. Do the records affect the interests of third parties?

5. Will there be a cost for processing the request?

6. Is a time extension required? If so, notify the requester [section 20].

7. Does it appear that you will be granting access to records that affect the interests of a third party? If so, send notices and give affected third parties an opportunity to make representations about the disclosure of records that affect them [section 21]. This will affect the deadline for responding to the request.

8. If the fee will be over $25.00, the requester must be given a fee estimate [subsection 45(3)].

Processing the Request

1. Retrieve the records.

2. Determine what exemptions apply [sections 6 - 15].

3. Determine if the override provisions apply [sections 5, 16].

4. If required, sever exempt material from the records.

5. Determine what the final fee will be and if the fees will be waived [section 45].

Granting or Denying Access to the Records

1. If access to a record or part of a record is granted, determine the method of access (copy or original) [section 23].

2. If access is granted, give the requester notice regarding access [section 19].

3. If an affected third party is involved, give notice regarding access to third party and requester [subsection 21(8)].

   Note that the affected third party has 30 days in which to appeal your access decision to the Commissioner. Access is not granted to the record until the 30 days have expired and an appeal has not been filed.

4. Collect fee where applicable, and provide record.

OR

Give the requester a *notice of refusal* if:

- the record does not exist;

- all or part of the record is exempt from disclosure; or

- you are refusing to confirm or deny the existence of certain records [section 22].

Correcting Personal Information

1. If an individual requests the correction of personal information, verify the information to be corrected, correct the personal information or permit a statement of disagreement to be filed.

2. If requested, notify recent users of the personal information of the correction or statement of disagreement [subsection 36(2)].

Complete the File

1. Document the request and all actions taken.

2. Close the file, unless an appeal is commenced.

CHAPTER 4

EXEMPTIONS

EXEMPTIONS

Introduction

The exemptions to access are set out in sections 6 to 15, and 38. The institution bears the burden of proving that an exemption is justified in the event of an appeal to the Commissioner [section 42].

Exemptions in sections 6 to 13 and section 15 apply to requests for access to general records. Exemptions in sections 14 and 38 apply to requests for access to personal information. The exemption in section 14 (personal privacy) applies to requests for access to another individual's personal information. The exemption in section 38 applies to a request by an individual for his or her own personal information . More than one exemption may apply to a requested record.

Some exemptions contain exceptions. Exceptions are provisions that limit the applicability of that particular exemption.

For example:

> Subsection 7(1) provides an exemption for advice and recommendations. However, subsection 7(2) provides exceptions to this exemption; a list of records that cannot be exempted under subsection 7(1).

Exceptions outlined in a section apply only to that section. However, another exemption may apply to a record.

Severability

Where an exemption applies to only part of a requested record, an institution must make available as much of the record as possible without disclosing the exempt portions [subsection 4(2)]. This is done by severing the exempt portions from the record before it is released. Information not described in or pertinent to the request may also be severed before the remainder is made available.

Procedures and methods of severing records are discussed in Chapter 3.

Mandatory and Discretionary Exemptions

There are two types of exemptions in the Act: mandatory and discretionary. Mandatory exemptions impose a duty on the head of an institution to refuse to disclose a record. Mandatory exemptions begin with the words "a head shall refuse to disclose...". The head must determine whether facts exist or may exist that bring the record within the exemption. If grounds for the exemption exist, the head must refuse access, unless a compelling public interest clearly outweighs the purpose of the exemption [section 16]. There are three mandatory exemptions:

- Relations with governments [section 9];
- Third party information [section 10]; and
- Personal privacy [section 14].

The remainder of the exemptions, sections 6, 7, 8, 11, 12, 13, 15 and 38, are discretionary. Discretionary exemptions permit the head to disclose a record despite the existence of the exemption. Discretionary exemptions are introduced by the words "a head may refuse to disclose...".

The Act requires a two-stage process in determining whether a discretionary exemption is to be applied. First, the head must determine whether the record falls within the exemption. Second, the head must decide whether he or she is willing to release the record, despite the existence of grounds for the exemption. A decision by a head to disclose information

falling within an exemption is an exercise of discretion.

The compelling public interest provision must be considered in the case of the discretionary exemption in section 7 (advice or recommendations), section 11 (economic and other interests) and 13 (danger to safety or health), if the head has decided not to exercise his or her discretion in favour of disclosure. See Chapter 3 for a discussion on compelling public interest.

Discretionary exemptions may be applied by the head alone. In an appeal situation, if a head chooses not to claim a discretionary exemption, no other party to the appeal may claim one.

Draft By-Laws, Records of Closed Meetings [Section 6]

Subsection 6(1)(a) is a *discretionary* exemption which permits the head to deny access to a draft by-law or private bill, unless the draft has been considered in an open meeting. The term *considered* involves examination or deliberation.

Subsection 6(1)(b) permits the head to prevent disclosure of a record which reveals the substance of deliberations of a closed meeting of a council, board, commission or other body or a committee of one of them. There must be statutory authority to hold the meeting in the absence of the public.

If the subject matter of the deliberations is later considered in an open meeting, this exemption no longer applies to the record.

The exemption in 6(1) cannot be relied on if the records mentioned in subsection 6(1)(a) or (b) are over 20 years old. Unless another exemption applies, the record must be released upon request.

The compelling public interest override in section 16 does not apply to this exemption.

Advice or Recommendations [Section 7]

Subsection 7(1) provides a *discretionary* exemption for records where disclosure would reveal the advice or recommendations of officers or employees of institutions or of consultants retained by an institution. Officers or employees include those persons who work for an institution or who perform duties under a contract of employment. The advice of an officer or employee of another institution cannot be exempted under this section, nor can advice of a volunteer.

The exemption is for advice or recommendations. There is some overlap between the terms advice and recommendations. *Recommendations* refers to formal recommendations about courses of action to be followed which are usually specific in nature and are proposed mainly in connection with a particular decision. *Advice* refers to less formal suggestions about particular approaches to take or courses of action to follow. The advice or recommendations must be communicated from one employee to another, and must be made in the course of the deliberative process of decision-making and policy--making. An employee's memo to file has not been communicated and would not be included in this exemption.

Subsection 7(1) is not restricted to advice or recommendations given to the head of the institution.

Subsections 7(2) and (3) provide **exceptions** to the exemption in subsection 7(1). Discussed immediately below are the types of records and information listed in subsections 7(2) and (3). A report or study in the following list means a completed document ready for presentation and would not include working papers used in

FIGURE III

EXEMPTIONS

SECTION	MANDATORY OR DISCRETIONARY	COMPELLING PUBLIC INTEREST PROVISION
s.6 Draft by-laws, records of closed meetings	Discretionary	No
s.7 Advice or recommendations	Discretionary	Yes
s.8 Law Enforcement	Discretionary	No
s.9 Relations with governments	Mandatory	Yes
s.10 Third party information	Mandatory	Yes
s.11 Economic and other interests	Discretionary	Yes
s.12 Solicitor-client privilege	Discretionary	No
s.13 Danger to safety or health	Discretionary	Yes
s.14 Personal information	Mandatory	Yes
s.15 Published information	Discretionary	No
s.38 Limitations on access to own personal information	Discretionary	No

preparation such as notes or preliminary drafts. For the types of records listed in subsection 7(2)(b) through (k), the record or part of it cannot be exempted under subsection 7(1), even if it contains advice or recommendations.

Factual Material
[Subsection 7(2)(a)]

Records or parts of records containing essentially factual material must be disclosed.

Factual material means a coherent body of facts which can be separated from the rest of the advice or recommendations, for example, an appendix of factual information supporting a policy document. Where factual material and advice or recommendations are contained in the same record, the advice or recommendations may be severed and withheld. However, it may not be possible to sever advice and recommendations and still leave meaningful factual information. In this circumstance, severing may not be appropriate, and the information would not be disclosed.

Statistical Survey
[Subsection 7(2)(b)]

A statistical survey must be disclosed unless another exemption applies.

A statistical survey is a record showing the collection, analysis, interpretation and presentation of aggregate data in relation to a topic or issue which is the object of study, for example, a poll. Any information identifying individuals must be removed before the record is disclosed.

Valuator's Report
[Subsection 7(2)(c)]

A valuator is someone with specific expertise appointed to determine or estimate the value, price or merit of an article. He or she need not be an officer of the institution. A valuator's report would include an appraisal of the value of real property.

Environmental Impact Statement
[Subsection 7(2)(d)]

An environmental impact statement or similar record must be disclosed.

An environmental impact statement is a record containing a technical assessment, including findings and conclusions respecting the social, cultural, economic and environmental consequences of projects such as buildings and highways.

Report on Performance
[Subsection 7(2)(e)]

A report or study on the performance or efficiency of an institution is not exempt under subsection 7(1).

For example:

> A final audit report, including its findings and conclusions would not be exempt.

Feasibility Study
[Subsection 7(2)(f)]

A feasibility or other technical study, including cost estimate, relating to a policy or project of an institution.

For a record to qualify as a feasibility study, it must be a study which is practicable, possible, capable of being done or accomplished and has a reasonable assurance of success.

For example:

> A feasibility study for a micrographics program would not be exempt.

Field Research Report
[Subsection 7(2)(g)]

The exemption in subsection 7(1) does not apply to a report setting out the findings and conclusions of field research on an issue or problem which is undertaken before the formulation of a policy proposal.

Proposal to Change or Establish a Program
[Subsection 7(2)(h)]

This subsection requires disclosure of a final plan or proposal to change or establish a program, including a budgetary estimate, whether or not the plan or proposal is subject to approval.

Subsection 7(2)(h) must be considered in relation to the exemption in subsection 11(f). Subsection 7(2)(h) refers to a final plan or proposal to alter or establish a program which provides a service to the public and which is developed or implemented to carry out the institution's responsibilities. Subsection 11(f) relates to internal administrative arrangements relating to personnel which do not fundamentally alter the nature and content of the programs being delivered to the public.

Committee Report
[Subsection 7(2)(i)]

A report of a committee within an institution must be disclosed unless another exemption applies to the record.

Report of a Body Attached to Institution
[Subsection 7(2)(j)]

The type of body referred to in this subsection is one that undertakes inquiries and makes reports or recommendations to the institution and consists primarily of representatives from outside the institution. The phrase *attached to an institution* indicates that the body has been appointed or invited to meet and deliberate by someone in an institution with appropriate authority.

For example:

> A local grants committee established to make recommendations regarding the awarding of grants would be one such body.

Reasons For a Final Decision
[Subsection 7(2)(k)]

Unless another exemption applies, this exception requires the disclosure of the reasons for a final decision, order or ruling by an officer or employee of the institution. This exemption applies regardless of whether or not the reasons are recorded in an internal memorandum or external correspondence.

Record More Than 20 Years Old
[Subsection 7(3)]

An institution must release a record that is more than 20 years old. This subsection does not place an obligation on an institution to retain a record for 20 years.

The compelling public interest provision in section 16 applies to this exemption.

Law Enforcement [Section 8]

Section 8 provides a *discretionary* exemption for records relating to police and by-law enforcement investigations and certain other investigative, adjudicative and protective functions.

Subsection 8(1) provides an exemption where disclosure could reasonably be expected to interfere with law enforcement and certain other activities. Subsection 8(2) exempts certain types of law enforcement records. Subsection 8(3) provides that a head may refuse to confirm or

deny the existence of records in subsections 8(1) and (2). Subsections 8(4) and (5) set out exceptions to the exemption.

Law enforcement is defined in subsection 2(1) of the Act. The phrase not only includes records relating to policing activities and prosecutions, but also records in respect of investigations, or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed. This definition encompasses records relating to the enforcement of federal and provincial statutes and municipal by-laws.

For example:

> The enforcement of property standards by-laws by a municipality or the enforcement of a no-smoking by-law by a transit authority would constitute a law enforcement activity.

The term *could reasonably be expected to* as used in this section requires that the expectation of the harm coming to pass should the record be disclosed, not be fanciful, imaginary or contrived, but based on reason. By virtue of section 42, an institution must provide evidence to substantiate the reasonableness of the expected harm.

Law Enforcement Matter [Subsection 8(1)(a)]

This exemption applies if disclosure could reasonably be expected to interfere with a law enforcement matter. To interfere with a law enforcement matter means that the disclosure would have the effect of hindering or impeding the conduct of a proceeding or the carrying out of a law enforcement activity.

Law enforcement matter refers to a proceeding or an activity that is within the scope of law enforcement as defined in subsection 2(1).

Law Enforcement Investigation [Subsection 8(1)(b)]

An institution may refuse to disclose a record where the disclosure could reasonably be expected to interfere with an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

To interfere with an investigation does not mean that disclosure would altogether prevent a law enforcement investigation from taking place but rather that disclosure would frustrate or impede the carrying out of an investigation.

Reveal Investigative Techniques [Subsection 8(1)(c)]

The purpose of this exemption is to preclude access to information about the application of technology to investigative techniques where disclosure would undermine or jeopardize the effectiveness of such techniques.

Reveal a Confidential Source [Subsection 8(1)(d)]

An institution may refuse to disclose a record where the disclosure would reveal the identity of a confidential source of information in respect of a law enforcement matter, or disclose information furnished only by the confidential source.

For example:

> A person who complains against his or her neighbour in respect of a municipal by-law infraction is a source protected under the exemption.

Safety of a Law Enforcement Officer [Subsection 8(1)(e)]

An institution may refuse to disclose a record that would endanger the safety of a law

enforcement officer or any other person.

Please see section 13, danger to safety or health, for further information.

Fair Trial or Impartial Adjudication [Subsection 8(1)(f)]

This exemption prevents premature disclosure of information that could deprive a person of a fair trial or impartial adjudication. Once the proceeding has been completely disposed of (including appeals), the exemption no longer applies.

This subsection does not contain a reference to law enforcement and, accordingly, the exemption applies to proceedings that do not fall within the definition of law enforcement such as tribunals established by legislation to adjudicate individual or collective rights. An example of such a tribunal would be the Social Assistance Review Board. To rely on this exemption, however, there must be evidence that the disclosure of the records would result in unfairness.

Intelligence Information [Subsection 8(1)(g)]

This subsection exempts from disclosure records where the disclosure could reasonably be expected to interfere with the gathering of or reveal law enforcement intelligence information respecting organizations or persons.

Confiscated Records [Subsection 8(1)(h)]

This exemption applies where disclosure could reasonably be expected to reveal records confiscated by a peace officer in accordance with an Act or regulation.

Endanger the Security [Subsection 8(1)(i)]

An institution may refuse to disclose a record where the disclosure could reasonably be expected to endanger the security of a building or the security of a vehicle carrying items, or of a system or procedure established for the protection of items, for which protection is reasonably required.

For example:

> A security audit is a record where disclosure would endanger the security of a system or procedure established for the protection of items.

Facilitate Escape [Subsection 8(1)(j)]

Records are exempt where the disclosure could reasonably be expected to facilitate escape from custody of a person who is under lawful detention. Custody indicates that an individual is not free to leave a place of confinement without restriction. In general, any person held in custody pursuant to a valid warrant or other authorized order is under lawful detention.

Centre for Lawful Detention [Subsection 8(1)(k)]

This provision exempts records where disclosure could reasonably be expected to jeopardize the security of a centre for lawful detention. This includes records containing details of previous investigations of escape attempts and details of security measures in place.

Unlawful Act [Subsection 8(1)(l)]

Records are exempt where the disclosure could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of a crime. Unlawful act means a

contravention of a statute or regulation or of a municipal by-law.

Other Law Enforcement Exemptions

Subsection 8(2) specifies certain records that the institution may refuse to disclose in response to a request. These records are described immediately below.

Law Enforcement Report
[Subsection 8(2)(a) and 8(4)]

Subsection 8(2)(a) exempts from disclosure a report prepared in the course of law enforcement inspections or investigations by an agency responsible for enforcing and regulating compliance with a law. Reports includes internal memoranda, complaint processing records and proposed witness statements. Agency includes organizations acting on behalf of or as agents for law enforcement agencies.

Subsection 8(2)(a), however, is modified by subsection 8(4), which does not allow the institution to exempt a routine inspection report. Routine inspections are carried out when there are no specific allegations that standards have been breached. Routine inspections include random inspections as well as those done on a regular basis. While the standards are frequently set out in a by-law or regulation, the statute provides the authority for enforcement and compliance.

For example:

> The *Fire Marshals Act* authorizes the Fire Chief to enforce compliance with fire safety standards through routine inspections. These standards are set out in the *Fire Marshals Act* and the *Ontario Fire Code* (R.R.O. 1990, Reg. 454). These inspections need not take place as a result of a complaint. The records of these routine inspections would not be exempt under subsection 8(2)(a).

Act of Parliament
[Subsection 8(2)(b)]

This subsection exempts a law enforcement record where disclosure would be an offence under an Act of Parliament.

For example:

> Section 46 of the *Young Offenders Act* makes it an offence to knowingly disclose certain court, police and government records relating to young offenders, except as authorized by that Act.

Civil Liability
[Subsection 8(2)(c)]

Subsection 8(2)(c) exempts a law enforcement record where disclosure could reasonably be expected to expose the author of the record, or any person who had been quoted or paraphrased in the record to civil liability.

The purpose of this exemption is to provide protection for law enforcement officials who might be sued for defamation as a result of disclosure of records made while carrying out their duties.

Correctional Authority
[Subsection 8(2)(d)]

Subsection 8(2)(d) exempts records that contain information relating to an individual's correctional history while the individual is under the control or supervision of a correctional authority.

Refusal to Confirm or Deny the Existence of a Record

Subsection 8(3) provides that a head may refuse to confirm or deny the existence of a record to which subsections 8(1) or 8(2) apply. Situations may arise in which merely disclosing the existence of an investigation or intelligence file

will communicate information to the requester which may impede ongoing investigation or intelligence-gathering.

Exceptions to Exemption for Law Enforcement

Routine Inspections [Subsection 8(4)]

This subsection requires an institution to disclose a record that is a report prepared in the course of routine inspections by an agency that is authorized to enforce and regulate compliance with a particular statute of Ontario.

For further discussion on routine inspections, see Law Enforcement Report [subsection 8(2)(a)].

Degree of Success in a Law Enforcement Program [Subsection 8(5)]

Subsection 8(5) provides that the exemptions in subsections 8(1) and (2) do not apply to a record regarding the degree of success achieved in a law enforcement program, unless the disclosure of such a record would prejudice, interfere with, or adversely affect any of the matters referred to in 8(1) or (2).

The compelling public interest override in section 16 does not apply to this exemption.

Relations with Governments [Section 9]

Section 9 provides a *mandatory* exemption where disclosure of a record could reasonably be expected to reveal information received in confidence from:

- the Government of Canada;
- the Government of Ontario;
- the government of another province or territory;
- the government of a foreign country or state; or
- an international organization of states (e.g., the United Nations).

Records received in confidence from agencies or boards of these governments would be included in this exemption.

If the government which supplied the confidential information consents to its release, the exemption does not apply. The Act does not require the institution to seek this consent, although in every case where this exemption is to be applied, the institution should consider whether it is appropriate to seek consent.

This exemption applies only to records received in confidence from the governments specified in section 9. This exemption does not apply to records received in confidence from another municipality or local board. The Act provides that the request can be transferred to the originating municipality or local board if that institution has the greater interest. See Chapter 3 for a discussion on this transfer provision.

The compelling public interest provision in section 16 applies to this exemption.

Third Party Information [Section 10]

Institutions often acquire information about the activities of businesses in the private sector. Some of this information may constitute a valuable asset to the company, and disclosure would impair its ability to compete effectively. Subsection 10(1) provides a *mandatory* exemption from disclosure for certain third party information where disclosure could reasonably be expected to cause certain harms. This exemption is not limited to commercial

third parties, but may also apply to any supplier of information which meets the tests specified below, including another institution.

Section 21 provides that before access is granted to a record that might contain information referred to in subsection 10(1) affecting the interests of a third party, that party must be notified and given the opportunity to make representations before a final access decision is made. If a third party claims in its representations that the record is exempt, the burden of establishing that the record falls within this section rests with that third party. Similarly, where an institution asserts that section 10 applies, the burden of proof is on the institution. Notification procedures are discussed in Chapter 3.

Before this exemption can be applied, *all* of the following three tests must be met:

- the information must fit within one of the specified categories of third party information;
- the information must have been *supplied* by the third party *in confidence,* implicitly or explicitly; and
- the disclosure of the information could reasonably be expected to cause certain harms specified in section 10.

The three tests are discussed in more detail immediately below.

Test #1: Categories of Third Party Information

Before subsection 10(1) applies, the record in question must contain one or more of the following types of information:

Trade secret: A trade secret must consist of information and may be used for an industrial, trade or business use. The trade secret is not generally known in that industry, trade or business and has economic value from not being generally known. It has also been treated in a manner to ensure its continued confidentiality.

Scientific information: This term refers to information relating to or exhibiting the principles of science.

For example:

> Scientific information would be contained in a proposal describing innovative energy technologies in a grant application.

Technical information: This term refers to information particular to an art or profession, for instance, architectural design or system design specifications.

Commercial information: This term refers to information concerning the sale, purchase, or exchange of goods, products or property.

For example:

> Customer and price lists, lists of suppliers, marketing and advertising plans, and similar information related to the commercial operation of a business would be commercial information.

Financial information: This term refers to information relating to money and its use or distribution.

For example:

> Cost accounting methods, pricing practices, profit and loss data, overhead and operating costs are all examples of financial information.

Labour relations information: This term refers to information concerning the relationship between employers and their employees, both

union and non-union, particularly information relating to collective bargaining.

For example:

> Records relating to the bargaining positions of an employer and a union engaged in mediation proceedings would be labour relations information.

Test #2: Supplied in Confidence

Subsection 10(1) provides that the information must be supplied in confidence. Information that is created or is gathered by the institution is not supplied by a third party and would not qualify for this exemption.

For example:

> A fee paid by an institution to a consultant is not supplied by the consultant; it is created by the institution.

The intention to maintain confidentiality may be expressed or may be implied by the circumstances (or the conduct of the parties). Confidentiality may be implied where there is evidence that the information was consistently treated in a confidential manner.

For example:

> Generally, material provided as a result of a sealed tender meets the confidentiality test where the written policy of the institution stipulates that confidentiality would be maintained.

Information that was available to interested parties and the general public before the Act was in force cannot be supplied in confidence.

Test #3: Harms Test

If the information falls within one of the categories described, and was supplied in confidence, it is then necessary to demonstrate that its disclosure could reasonably be expected to yield one of the results listed in subsections 10(1)(a), (b), (c), or (d).

Competitive Position or Negotiations [Subsection 10(1)(a)]

This subsection applies where the disclosure could reasonably be expected to prejudice significantly the competitive position or interfere with the contractual or other negotiations of a person or organization (whether or not the person or organization is the third party submitting the information).

The institution or third party must present evidence that is detailed and convincing and must describe a set of facts and circumstances that would lead to a reasonable expectation that harm would occur if the information were released. Generalized statements of fact without sufficient evidence do not meet the test.

Information No Longer Supplied [Subsection 10(1)(b)]

This subsection applies where the disclosure could reasonably be expected to result in similar information no longer being supplied to an institution where it is in the public interest that similar information continue to be supplied.

This provision would not apply where the information is submitted voluntarily in an application for a benefit or a grant, or where a statute requires the provision of this information.

The test is whether the third party or another source would entrust similar information to the institution in the future if the information were disclosed. If not, this subsection applies.

Undue Loss or Gain [Subsection 10(1)(c)]

This subsection applies where the disclosure could reasonably be expected to result in undue loss or gain to any person or organization. Undue means more than necessary, excessive, or unjustified.

Labour Relations Information [Subsection 10(1)(d)

This subsection applies where the disclosure could reasonably be expected to reveal information supplied to or the report of a conciliation officer, mediator, labour relations officer or other person appointed to resolve a labour relations dispute.

Exception to Exemption for Third Party Information [Subsection 10(2)]

Subsection 10(2) provides an exception to the exemption in subsection 10(1) where the affected third party consents to disclosure. While the institution need not seek the consent of the third party in each case, he or she is required to *consider* whether the consent ought to be sought.

The compelling public interest provision in section 16 applies to this exemption.

Economic and Other Interests [Section 11]

Section 11 provides a *discretionary* exemption for certain proprietary information of institutions and the premature disclosure of certain plans or negotiating strategies. Information affecting the interests of third parties is covered by section 10.

Subsections 11(a) through (g) set out the types of information and circumstances covered by this exemption.

Commercial Information [Subsection 11(a)]

This subsection allows the institution to refuse access to trade secrets, or financial, commercial, scientific or technical information belonging to an institution and has monetary value or potential monetary value. These terms have the same meaning as in subsection 10(1), described above. The information may belong to the institution receiving the request or to another institution.

Having monetary value or potential monetary value means that the trade secret or information is or is potentially marketable.

Employee Research [Subsection 11(b)]

This subsection exempts information obtained through research by an employee of an institution where the disclosure could reasonably be expected to deprive the employee of priority of publication. The employee must intend to publish the information.

Economic Interests [Subsection 11(c)]

This subsection exempts information where the disclosure could reasonably be expected to prejudice the economic interests or competitive position of an institution.

Economic interests concern the production, distribution and consumption of goods and services. If it can be reasonably expected, for instance, that disclosure of certain information would cause an institution to pay a higher price for goods and services, that information may be exempt under subsection 11(c).

Competitive position applies only to those institutions engaged in the supply of goods and services on a competitive basis.

Financial Interests
[Subsection 11(d)]

This subsection exempts information where the disclosure could reasonably be expected to be injurious to an institution's financial interests.

Financial interests refers to an institution's financial position, its ability to collect taxes and generate revenues, and its ability to protect its own interests in financial transactions with third parties.

Negotiating Strategy
[Subsection 11(e)]

An institution may refuse to disclose positions, plans, procedures, criteria or instructions concerning negotiations carried on by or on behalf of an institution.

Negotiations in this subsection mean discussions and communications where the intent is to arrive at a settlement or agreement. This exemption applies to on-going and future negotiations.

Personnel or Administration Plans
[Subsection 11(f)]

An institution may refuse to disclose plans relating to the management of personnel or the administration of an institution. This subsection is intended to cover the internal management plans of an institution, such as a reorganization or relocation prior to implementation. See subsection 7(2)(h) above which concerns proposals to change or establish a public program.

Once the plan has been put into operation or made public, subsection 11(f) does not apply.

Policy Decisions/Unfair Advantage
[Subsection 11(g)]

This subsection exempts information such as proposed plans, policies or projects where the disclosure could reasonably be expected to result in:

- premature release of a pending policy decision; or
- undue financial benefit or loss to a person.

There must be evidence to support the assertion that one of the two specified results would occur.

Examination or Test Questions
[Subsection 11(h)]

An institution may refuse to disclose questions that are to be used in an examination or test for an educational purpose. Once the question is no longer to be used in an exam or test, the exemption does not apply.

Questions for a job competition are not included in this exemption.

Submissions Under the Municipal Boundary Negotiations Act
[Subsection 11(i)]

This subsection exempts records containing submissions made under the *Municipal Boundary Negotiations Act*, by a party municipality or other body. This exemption may be only be invoked before the matter is resolved under the Act.

The compelling public interest provision in section 16 applies to this exemption.

Solicitor-client Privilege [Section 12]

Section 12 is a *discretionary* exemption relating to records which are subject to the solicitor-client privilege. All communications of a confidential nature between an institution and its legal advisor directly related to legal advice are covered. This includes working papers and statements of the legal advisor's account with the client. For solicitor-client privilege to apply, four criteria must be met:

- there must be a written or oral communication;
- the communication must be of a confidential nature;
- the communication must be between an institution and a legal advisor; and
- the communication must be directly related to seeking, formulating or giving legal advice.

Papers and materials created or obtained especially for the lawyer's brief for existing or contemplated litigation are privileged, whether or not the information has been communicated to or from the client.

Also included are records prepared by or for counsel employed or retained by an institution for use in giving legal advice or in contemplation of or for use in litigation.

While only the client may waive the privilege, all circumstances regarding the disclosure of a legal opinion must be considered to determine whether there has been a waiver.

For example:

> If a client disclosed an opinion to a specific party, intentionally and without any restrictions on its use, the release could constitute a waiver of the solicitor-client privilege.

Institutions must take care to ensure that legal opinions are not released to a specific party as the solicitor-client privilege may be jeopardized. If an institution wishes to release privileged information to a specific party, it should place restrictions on its use to retain the solicitor-client privilege.

The compelling public interest provision in section 16 does not apply to this exemption.

Danger to Safety or Health [Section 13]

Section 13 provides a *discretionary* exemption relating to records, the disclosure of which could reasonably be expected to seriously threaten the safety or health of any individual.

This exemption is not intended to restrict an individual's right of access to his or her own personal information, except where disclosure could threaten the safety or health of another individual.

The compelling public interest provision in section 16 applies to this exemption.

Personal Privacy [Section 14]

Subsection 14(1) provides a *mandatory* exemption relating to the disclosure of personal information to an individual other than the individual to whom the information relates. Section 14 is one of the keystone provisions of the Act. It balances the public's right of access to records and the individual's right of privacy respecting personal information.

Subsection 14(1) requires the institution to refuse to disclose personal information, unless

one of the circumstances listed in 14(1)(a) through (f) apply.

Subsections 14(2)(a) through (i) lists circumstances which should be considered in determining whether a disclosure of personal information constitutes an unjustified invasion of personal privacy.

Subsection 14(3) sets out circumstances where disclosure is presumed to be an unjustified invasion of personal privacy.

Subsection 14(4) lists when disclosure does not constitute an unjustified invasion of personal privacy.

Subsection 14(5) permits an institution to refuse to confirm or deny the existence of a record if its disclosure would constitute an unjustified invasion of privacy.

Where an institution has reason to believe that a disclosure might constitute an unjustified invasion of personal privacy, section 21 provides that an institution must give notice to the person to whom the personal information relates before granting access to a record. This person must be given the opportunity to make representations about the disclosure. See **Notices to Affected Third Parties** in Chapter 3.

Exceptions to Exemption for Personal Privacy

Subsection 14(1)(a) through (f) outlines circumstances when personal information may be disclosed to someone other than the individual to whom the information relates.

Consent [Subsection 14(1)(a)]

Personal information can be disclosed to someone other than the individual to whom the information relates with the prior request or consent of the individual. The record must be one to which the individual is entitled to have access.

The request or consent should be in writing and be received before the personal information is disclosed.

Compelling Circumstances [Subsection 14(1)(b)]

Personal information may be disclosed to a person other than the individual to whom the personal information relates in compelling circumstances affecting the health or safety of an individual.

Circumstances are *compelling* when either there is no other way to obtain personal information affecting health or safety, or there is an emergency situation where the delay in obtaining the information would be injurious to someone's health or safety. The determination of when compelling circumstances exist is left to the discretion of the head.

Where personal information is released under this subsection, upon disclosure, notification must be mailed to the last known address of the individual to whom the information relates. If the institution does not have the address, it must attempt to find out the address of the individual from the person who made the request.

Public Records [Subsection 14(1)(c)]

Personal information may be disclosed to another person in response to a request made under the Act if the personal information is collected and maintained specifically for the purpose of creating a record available to the general public.

A public record refers to a collection of personal information to which all members of the public have equal access.

See Chapter 5 for further discussion of public records.

Disclosure Expressly Authorized by Statute [Subsection 14(1)(d)]

Personal information may be disclosed to a person other than the individual to whom the personal information relates where an Act of Ontario or Canada expressly authorizes disclosure.

For example:

> Personal information may be released to an individual other than the individual to whom the personal information relates pursuant to the Unemployment Insurance Act, subsection 94(11). This subsection expressly authorizes disclosure of personal information to the Unemployment Insurance Commission.

Research Agreements [Subsection 14(1)(e)]

An institution may disclose personal information in response to a request under the Act, if the disclosure is for a research purpose, when certain conditions are met. *Research purposes* are distinct from administrative, operational or regulatory uses of personal information in that research uses do not directly affect the individual to whom the information relates and do not relate to the usual administration of a program.

This provision covers disclosures to researchers receiving grants, consultants conducting contractual research and independent researchers. Access to personal information by researchers who are employees of an institution is covered by section 31 and subsection 32(d), and not subsection 14(1)(e).

The institution must determine that conditions are appropriate for the disclosure of personal information for a research purpose. The following conditions must be met:

- the disclosure must be consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained. If the information was provided with a reasonable expectation of confidentiality, access should not be granted without the consent of the individual;
- the research purpose for which the disclosure is to be made cannot be reasonably achieved unless the information is provided in a form which allows individuals to be identified;
- the researcher must comply with conditions relating to security and confidentiality prescribed by the regulations. See section 10 of R.R.O. 1990, Reg 823 for a list of these conditions; and
- the disclosure is not an unjustified invasion of privacy [subsection 14(1)(f)].

Unjustified Invasion of Personal Privacy [Subsection 14(1)(f)]

Access to another individual's personal information may be granted where the disclosure does not constitute an unjustified invasion of personal privacy. This is determined by balancing the factors set out in subsections 14(2) and 14(3).

Factors to be Considered

In determining whether disclosure of personal information to someone other than the person to whom it relates constitutes an unjustified invasion of privacy, the institution must consider all the relevant circumstances.

The circumstances listed in subsections 14(2)(a) through (i) should be considered in deciding whether or not to disclose personal information.

Some may rebut the presumption in subsection 14(3) that release of the personal information would invade an individual's privacy; that is, the record could be disclosed. However, some of the enumerated circumstances in subsection 14(2) reinforce the presumptions in subsection 14(3) and favour a denial of access.

The list in subsection 14(2) is not exhaustive; any other relevant circumstances should be considered by the institution before a decision on disclosure is made.

Public Scrutiny
[Subsection 14(2)(a)]

In determining whether disclosure constitutes an unjustified invasion of personal privacy, an institution must consider whether disclosure is desirable for subjecting the activities of the institution to public scrutiny.

The institution should consider the broader interests of public accountability. Invoking this provision should not be limited to instances where it is alleged that the institution's normal practices or procedures were not followed.

Public Health and Safety
[Subsection 14(2)(b)]

One of the relevant circumstances the institution must consider in determining whether disclosure constitutes an unjustified invasion of personal privacy is if access to the personal information may promote public health and safety.

Informed Choice
[Subsection 14(2)(c)]

In determining whether disclosure constitutes an unjustified invasion of personal privacy, an institution must consider whether disclosure will promote informed choice in the purchase of goods and services.

For example:

> Disclosure of an evaluation of a supplier's or consultant's performance could disclose personal information.

Fair Determination of Rights
[Subsection 14(2)(d)]

In determining whether disclosure constitutes an unjustified invasion of personal privacy, an institution must consider whether the personal information is relevant to a fair determination of the requester's rights. There may be instances where the requester requires access to personal information about someone else in order to assist the requester in obtaining a determination of his or her rights.

For example:

> Records in respect of an investigation of alleged sexual harassment may be released to the person against whom the allegation is made, in the absence of other factors. One factor leading to non-disclosure might be evidence of potential harm to witnesses if their identities were disclosed.

Unfair Exposure to Harm
[Subsection 14(2)(e)]

The institution must consider whether the individual will be exposed unfairly to pecuniary or other harm.

This consideration is relevant only where there is evidence that unfair pecuniary or other harm will result from the disclosure.

Highly Sensitive Information
[Subsection 14(2)(f)]

One of the relevant circumstances the institution must consider in determining whether disclosure constitutes an unjustified invasion of personal privacy is if the information is highly sensitive.

Information Inaccurate or Unreliable [Subsection 14(2)(g)]

The institution must consider whether the personal information is unlikely to be accurate or reliable.

Subsection 30(2) requires institutions to take reasonable steps to ensure that personal information is not used unless it is accurate and up to date.

Information Supplied in Confidence [Subsection 14(2)(h)]

In determining whether disclosure constitutes an unjustified invasion of personal privacy, an institution must consider whether the personal information was supplied by the individual to whom it relates in confidence.

This subsection does not apply to information supplied in confidence by one individual about another.

Damage to Reputation [Subsection 14(2)(i)]

In determining whether disclosure constitutes an unjustified invasion of personal privacy, an institution must consider whether disclosure may unfairly damage the reputation of any person referred to in the record.

Presumed Invasion of Privacy

Subsection 14(3) provides that disclosure of certain types of personal information is presumed to be an unjustified invasion of personal privacy. These factors must be considered in conjunction with those listed in subsection 14(2) above to determine if the disclosure of personal information may be considered an unjustified invasion of privacy.

Medical Record [Subsection 14(3)(a)]

Disclosure of information that relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation is presumed to constitute an unjustified invasion of personal privacy.

Violation of Law [Subsection 14(3)(b)]

Disclosure of personal information compiled as part of an investigation into a possible violation of law is presumed to constitute an unjustified invasion of personal privacy.

For example:

> Personal information relating to sexual harassment investigations compiled by, or on behalf of, the Ontario Human Rights Commission are records compiled as part of an investigation into a possible violation of law. However, where internal investigations are conducted by an institution's human resources staff, this provision does not apply. The fact that a complainant *might* take their concerns to the Ontario Human Rights Commission does not alter the fact that this type of internal investigation does not have a possible violation of law.

This exemption does not apply where disclosure is necessary to prosecute the violation or to continue the investigation.

Eligibility for Social Programs [Subsection 14(3)(c)]

Disclosure of information that relates to eligibility for social service or welfare benefits is presumed to constitute an unjustified invasion of personal privacy.

Employment or Educational History [Subsection 14(3)(d)]

Disclosure of information that relates to an individual's employment or educational history is presumed to constitute an unjustified invasion of personal privacy. This presumption does not apply to employment-related duties or to employee expense claims.

Tax Return [Subsection 14(3)(e)]

Disclosure of personal information obtained on a tax return or gathered for the purpose of collecting a tax is presumed to constitute an unjustified invasion of personal privacy.

Financial History [Subsection 14(3)(f)]

Disclosure of personal information describing an individual's finances, income, assets, liabilities, net worth, bank balances, financial history or creditworthiness is presumed to constitute an unjustified invasion of personal privacy.

Specific salaries of individuals are personal information that must be protected, however, disclosure of a salary range is not considered an unjustified invasion of personal privacy.

Personal Recommendations and Evaluations [Subsection 14(3)(g)]

Disclosure of personal information consisting of personal recommendations or evaluations, character references, personnel evaluations is presumed to constitute an unjustified invasion of personal privacy.

Race, Ethnic Origin, Religion or Sexual Orientation [Subsection 14(3)(h)]

Disclosure of personal information which reveals an individual's racial, ethnic origin, religious or political beliefs or sexual orientation is presumed to constitute an unjustified invasion of personal privacy.

Exceptions to the Exemption

Despite the other provisions of section 14, subsection 14(4) lists two types of personal information where disclosure does not constitute an unjustified invasion of privacy.

Salary Range and Benefits of Employees [Subsection 14(4)(a)]

Disclosure of the classification, salary range and benefits, or employment responsibilities of an officer or employee of an institution is not an unjustified invasion of personal privacy. Note that the provision refers to *salary range*, not specific salary.

Officer or employee includes appointed officials and those persons who work for an institution, or who perform their duties under a contract of employment.

Personal Service Contracts [Subsection 14(4)(b)]

Disclosure of the financial or other details of a contract for personal services between an individual and an institution is not an unjustified invasion of privacy. A contract in which an individual, not a company, is hired to perform professional services in respect of a particular problem or project would be included.

Refusal to Confirm or Deny

Where the head refuses to give access to a record on the grounds of an unjustified invasion of privacy, the head may also refuse to confirm or deny the existence of the record. Where the head refuses to confirm or deny the existence of a record in response to a request, notification to the requester under subsection 22(2) is required.

FIGURE IV

Guide to Decision Under Section 14

Request for another individual's personal information

↓

s. 14(1)
Does an exception apply, i.e. s.14(1)(a) - (e) or s.14(4)?
- If so, release record
- If not, consider s.14(3)

↓

s. 14(3)
Presumed unjustified invasion of privacy if record released?

"YES"

If presumed invasion of privacy under s.14(3), are there any grounds in s.14(2) which rebut or modify this presumption?
- If yes, commence third party notice process s.21
- If no, record not disclosed

"NO"

If not presumed invasion of privacy under s.14(3), are there any grounds (inc. s.14(2)) to indicate disclosure would be unjustified invasion?
- If yes, record not disclosed
- If no, commence third party notice proceedings

Compelling Public Interest

Members of the public often wish to know some information about elected officials and appointees to public positions on boards and committees. Institutions are encouraged to prepare brief biographies, making them available to the public upon request, however the elected official or appointee should be made aware of this practice prior to publishing the biography.

See Appendix VI for a sample biography.

The compelling public interest provision in section 16 applies to this exemption.

Published Information [Section 15]

Section 15 is a *discretionary* exemption that allows an institution to refuse disclosure of a record where:

- the record or the information contained in the record has been published or is currently available to the public; or
- there are reasonable grounds to believe that the record or information will be published by the institution within 90 days of the request, or within a further period of time needed for printing the material or for translating it before printing.

This exemption is not limited to information published only by the institution. An institution has a duty to inform a requester where the record or information in question is available. Where an institution invokes this exemption, it must consider the convenience of the requester compared to the convenience of the institution.

Where an institution is faced with an important issue, generating numerous requests over a long period of time, and the institution will grant access to these records, it may be advantageous for the institution to put together a package of information and have it published. The institution could set a reasonable fee for the package.

The compelling public interest exemption in section 16 does not apply to this exemption.

Limitations on Access to One's Own Personal Information [Section 38]

While all of the exemptions discussed above are in Part I of the Act (Freedom of Information), section 38 falls in Part II (Protection of Individual Privacy).

In Part II, section 36 establishes a right of access to one's own personal information. Section 38 is a *discretionary* exemption to that right of access and sets out grounds for refusing to disclose personal information to the individual to whom the information relates.

General Exemptions [Subsection 38(a)]

This subsection provides that an individual's right of access to his or her own personal information is subject to the exemptions applying to general information. This includes the exemptions in sections 6 through 13, and section 15, but not section 14 which applies to the disclosure of an individual's personal information to a third party.

Unjustified Invasion of Another's Personal Privacy [Subsection 38(b)]

An institution may refuse to disclose to an individual his or her own personal information where the disclosure would constitute an unjustified invasion of another individual's personal privacy. Subsections 14(2) and (3)

provide the test for determining an unjustified invasion of personal privacy and guidance in interpreting this subsection.

There may be personal information about more than one individual in the same record. Severing may not be feasible because close family or business ties would allow individuals other than the requester to be identified despite severing. Therefore, if disclosure would invade the personal privacy of an individual other than the requester, disclosure may be refused.

There is a requirement for notification to the individual whose personal privacy may be invaded where release is contemplated. See **Notices to Affected Third Parties** in Chapter 3.

Revealing a Confidential Source [Subsection 38(c)]

The institution may refuse to disclose to an individual his or her own personal information when it is evaluative or opinion material where disclosure would reveal the identity of a source who furnished information to the institution. The information must have been provided in circumstances where it may reasonably have been assumed that the identity of the source would be held in confidence. The evaluative or opinion material must be compiled solely for the purpose of determining suitability, eligibility or qualifications for employment, or for the awarding of contracts and other benefits.

The information to which the exemption applies is only that information which would reveal the identity of the source. The phrase *information furnished to the institution* indicates that the source is someone outside the institution.

Medical Information [Subsection 38(d)]

The institution may refuse to disclose to an individual his or her own personal information where the disclosure could reasonably be expected to prejudice the individual's mental or physical health. This provision is intended where disclosure would be injurious to the individual. It is not intended as a general provision for withholding access to medical information. Wherever possible, an individual should be granted access to his or her medical information.

An institution may wish to consult with a medical practitioner or other appropriate professional to determine whether there is a reasonable expectation of prejudice to the individual's mental or physical health. When the information is disclosed to the requester, the medical practitioner or other appropriate professional may be present to provide explanations and to answer questions.

Research or Statistical Record [Subsection 38(e)]

An institution may refuse to disclose to an individual his or her own personal information if the personal information is collected for a research or statistical purpose not directly affecting the individual. If the information is used for any other purpose, this exemption does not apply.

CHAPTER 5

PRIVACY PROTECTION

PRIVACY PROTECTION

Introduction

One of the key principles of the *Municipal Freedom of Information and Protection of Privacy Act* is the protection of personal privacy. The requirements of the Act concerning personal privacy are set out in Part II, and include:

- establishing standards for the collection, use and disclosure of personal information by institutions;
- requiring that personal information records are retained and disposed of in such a way that the confidentiality of the records is maintained at all times.

The requirements of Part II restrict the collection, use and disclosure of personal information to the circumstances outlined in this chapter.

Public Records [Section 27]

Section 27 states that the provisions of Part II of the Act (sections 28 to 38) do not apply to personal information maintained for the purpose of creating a record that is available to the general public.

Public records of personal information are usually established under a statute, and are records to which all members of the public have equal access. Personal information to which some members of the public have access, while others do not, is not a public record for the purposes of the *Municipal Freedom of Information and Protection of Privacy Act.*

For example:

> A public record is a list of electors as required by section 28 of the *Municipal Elections Act*.
>
> Assessment rolls, as required by section 39 of the *Assessment Act*, are public records.

Collection of Personal Information [Sections 28 and 29]

This section expands the definition of personal information for the purpose of collection and sets out the authority for the collection of personal information.

Expanded Definition of Personal Information [Subsection 28(1)]

For the purposes of section 28 and 29, the definition of personal information found in section 2 of the Act is expanded to include non-recorded personal information.

For example:

> Personal information may be collected orally in a job interview. Although such information may not be recorded, the same rules regarding the collection of personal information apply.

When personal information is collected orally, it is very often a good business practice to make some written record that the information was received. There is no requirement in the Act, however, that such a record be created.

Authority to Collect [Section 29]

This subsection sets out the conditions under which personal information may be collected. Personal information is collected by an institution when the institution actively acquires the information or invites an individual or others to send personal information to the institution. An individual may submit personal information on

his or her own initiative without the information being requested by the institution. Receipt of this information is not considered a collection unless the institution keeps or uses the information.

For example:

Unsolicited resumes which are sent to an institution and are not in response to a job advertisement or competition are not collected. Resumes submitted in response to a job call are collected by the institution and authorization for collection is subject to subsection 29(1).

One of three conditions must exist in order for personal information to be collected:

- the collection of personal information is expressly authorized by a statute;
- the information collected is used for the purposes of law enforcement; or
- the collection is necessary for the proper administration of a lawfully authorized activity.

For example:

Personal information collected to develop a list of electors under section 21 of the *Municipal Elections Act* is a collection authorized specifically by a statute.

Information collected by social services investigators in the course of an investigation into social assistance fraud, is a collection for the purpose of law enforcement.

An activity is lawfully authorized when it is established by a statute, regulation or by-law. A collection of personal information on an application for a municipal business licence is necessary to the proper administration of the licensing of businesses.

By implication, the authority to collect personal information is limited to the collection of necessary information.

Manner of Collection [Subsection 29(1)]

This subsection requires that personal information be collected directly from the individual to whom it relates, unless certain circumstances described in subsections 29(1)(a) through (h) permit an indirect collection.

Individual Authorization [Subsection 29(1)(a)]

An individual may authorize an indirect collection of personal information. Such authorization should generally include:

- the identification of the personal information to be collected;
- the source from which the personal information may be collected; and
- the name of the institution that is to collect the personal information.

A record should be kept with the date and the details of the authorization.

Notice of the collection should be given to the individual concerned at the same time as the authorization is obtained. Notice of collection of personal information is discussed later in this chapter.

Disclosure Under Section 32 [Section 29(1)(b)]

Personal information may be collected by one institution from another institution where the disclosing institution has authority to disclose under section 32 of the *Municipal Freedom of Information and Protection of Privacy Act* or

section 42 under the *Freedom of Information and Protection of Privacy Act*.

For example:

> Under section 4(2) of the *General Welfare Assistance Act,* a municipality may collect personal information for the purpose of determining eligibility for welfare benefits.

When a welfare recipient moves to another municipality, the municipality originally providing benefits may disclose certain personal information about the recipient to the second municipality, so that the client's eligibility for welfare may be determined.

The disclosure is authorized by subsection 32(c) of the *Municipal Freedom of Information and Protection of Privacy Act,* as the disclosure to the second municipality is for the same or similar purpose for which the information was originally collected, namely, determining eligibility for welfare benefits. The second municipality, therefore, may collect the information since it has been properly disclosed to it under subsection 32(c) of the Act.

Authority of the Commissioner
[Subsection 29(1)(c)]

The Commissioner may authorize a collection from a source other than the individual. The Commissioner's authorization may be sought because the indirect collection is not specifically allowed under subsection 29(1), or where the institution believes it is not possible or practical to collect the personal information directly or to obtain authorization directly from the individual concerned under subsection 29(1)(a). Subsection 46(c) provides this power to the Commissioner.

Consumer Reporting Act
[Subsection 29(1)(d)]

This subsection authorizes an institution to collect personal information contained in a consumer report that is prepared in accordance with the *Consumer Reporting Act.* A complete list of information which may be included in such a report is contained in subsection 8(1)(d) of the *Consumer Reporting Act.*

Honour or Award
[Subsection 29(1)(e)]

This subsection authorizes an institution to collect personal information indirectly for the purpose of determining suitability for an honour or award to recognize outstanding achievement or distinguished service.

For example:

> Personal information can be collected to determine which of a number of candidates should receive a Citizen of the Year award.

Courts and Tribunals
[Subsection 29(1)(f)]

This subsection authorizes an institution to collect personal information indirectly for the conduct of a proceeding or a possible proceeding before a court or judicial or quasi-judicial tribunal.

A judicial or quasi-judicial tribunal is a body constituted under a statute with power to decide the legal rights of a person or the eligibility of a person for a benefit or licence. Such tribunals are required to adhere to standards of procedural fairness similar to the procedures of courts.

Examples of this type of tribunal include the Ontario Municipal Board, Property Standards Committee, Assessment Review Court, Social Assistance Review Board, Courts of Revision, and Committees of Adjustment.

In some cases, after personal information has been collected, no proceeding takes place

because, for example, there is insufficient evidence. Even though the tribunal may never hear the matter, this subsection applies as long as the purpose of the collection is to determine whether a proceeding can be commenced before a court or tribunal.

Law Enforcement
[Subsection 29(1)(g)]

Personal information which is collected for the purpose of law enforcement may be collected from a source other than the individual about whom the information relates. Law enforcement is defined in section 2(1) of the Act.

Statutory Authority
[Subsection 29(1)(h)]

A statute, regulation or by-law may authorize a collection of personal information from a source other than the individual.

For example:

> Under section 6(4) of the *Municipal Health Services Act,* a municipal assessment commissioner may require any employer to furnish a list of employees residing in the municipality, and the dates upon which the employees are paid their salary or wages.
>
> A municipality may pass a lodging licence by-law authorizing the municipality to conduct reference checks as part of its approval of an application for a lodging licence.

Notification Requirements [Subsection 29(2)]

When personal information is collected by an institution, either directly from the person about whom the information relates or indirectly from another source, the institution must inform the individual that the collection has occurred.

The notice to the individual must state:

- the legal authority for the collection;
- the principal purpose(s) for which the personal information will be used;
- the title, business address and telephone number of an official of the institution who can answer the individual's questions about the collection.

The notice of legal authority should include a reference to the specific act and section, or by-law which authorized the collection. Where an act or by-law does not specifically refer to the collection, then the notice should refer to the specific section of the act or by-law which establishes the activity or program under which the information is collected.

For example:

> Subsection 58(2) of the *Education Act* provides for the establishment of Boards of Education. Even though the *Education Act* may not specifically authorize each collection of personal information undertaken by a Board of Education, nonetheless subsection 58(2) of the *Education Act* would provide sufficient statutory authority to undertake collections of personal information that are *necessary to the functioning of a board.*

The statement regarding the principal purpose(s) for which the information will be used should be consistent with the allowable uses of personal information in section 31 of the Act. The principal purpose(s) for which the information will be used should also be consistent with the statement in the index of personal information banks which describes the use and disclosure of personal information in each bank (see section 34 of the Act and Chapter 2 of the Handbook).

Where the personal information is collected directly from the individual, notice should be

FIGURE V

Privacy Protection

Collection

- Authority to collect? [s.28(2)]
- Direct notification? [s.29(1)]
- Notification of collection? [s.29(2)]

Use

- Accurate and up-to-date? [s.30(2)]
- With consent? [s.31(a)]
- For consistent purpose? [s.31(b)]
- For the purpose disclosed? [s.31(c)]
- New use? If so, document new use? [s.35]

Disclosure

- Accurate and up-to-date? [s.30(2)]
- With consent? [s.32(b)]
- For consistent purpose? [s.32(c)]
- Other specific circumstances? [s.32(d) - (l)]
- New disclosure? If so, document new disclosure? [s.35]

Retention and Disposal

- Personal information secure and protected throughout retention and during disposal?
- Minimum retention period as established by regulation?

Personal Information Banks

- All personal information banks identified and described? [s.34(1)]
- Descriptions available to public? [s.34(1)]
- Descriptions accurate, including new regular uses and disclosures? [s.34(2)]

given to the individual at the time of the collection. Where the personal information is collected on a form, the notice may be provided on the form itself.

A notification should be included on a form where the principal purpose of the form is to collect personal information and the information is used for the purpose of making a decision affecting the individual.

A notification on an application for employment form might read as follows:

> Personal information contained on this form is collected under the authority of bylaw #XXX, and will be used to determine eligibility for employment. Questions about this collection should be directed to: Manager of Personnel [or other official] 123 Maple Street, Anytown, Ont. (123) 456-7890.

Forms which are prescribed by a provincial regulation are not controlled by a municipality or local board. In cases where personal information is collected on a prescribed form, it is the responsibility of the provincial ministry controlling the form to include a notice on the form.

Alternative ways of providing notice of collection could include:

- providing notice through public advertisement in the press (eg. where a public advertisement solicits the collection);
- orally informing the individual in the course of an in-person or telephone interview (and noting this in the individual's file); or
- including the notice in correspondence or as an insert with other mailed material.

Where personal information is collected and will be used by or disclosed to another institution, the individual should be given notice of:

- the legal authority that the first institution has for collecting the information;
- the principal purposes for which the personal information will be used by that institution;
- the address and telephone number of an official in that institution who can answer questions; and
- the fact that the information will be used by a second institution and the name of that institution.

If the individual is not informed at the time of collection that the information will be used by another institution, then the second institution must provide notice to the individual.

Where indirect collection is permitted under subsection 29(1), notice to the individual is still required.

Exception to Notice Requirements

Subsection 29(3) provides that notice of collection of personal information is not required if:

- the type of information being collected would be exempt from access under subsection 8(1) or 8(2) (law enforcement);
- the Minister (Chairman of the Management Board of Cabinet) waives the notice. Each request for a waiver is considered on its own merits. Waivers will normally be requested for a class or group of individuals rather than one individual; or
- the regulations provide that the notice is not required.

The regulations provide that notification is not required where:

- Notice Frustrates Purpose of the Collection:

In some cases, providing notice to the individual when personal information is collected may undermine the purpose for which the personal information is collected. An institution might collect personal information to determine the whereabouts of someone who is indebted to the institution and who has absconded to avoid paying the debt. In such circumstances, providing notice would frustrate the purpose of collecting the personal information, since notifying the debtor could result in the debtor taking further steps to avoid payment.

- Unjustified Invasion of Another Individual's Personal Privacy:

  Under the Act a notice of collection of personal information must describe how the information will be used. When the use touches upon sensitive personal matters involving another person, the notice may reveal personal information about another individual. An individual who applies for social assistance benefits from a municipality may be required to furnish the names and routine biographical details of the applicant's dependents or co-habitors. Providing notice to the dependents or co-habitor that personal information about them has been collected for the purpose of assessing the applicant's application would reveal sensitive personal information, namely that the individual has applied for assistance.

- Suitability or Eligibility for Award or Honour:

  An institution may collect the names and biographical details of persons to be considered for an award or honour. Where personal information about a candidate is collected for this purpose, a notice of collection of personal information is not required.

The head of the institution must make available to the public, a statement describing the purpose of the collection of personal information and the reason that notice has not been given. The statement should:

- identify the program or activity for which the personal information is collected;
- describe in general terms the type of personal information collected, and how the information will be used;
- state the time period during which the notice would not be given, for example, whether the notice is being dispensed with for a one-time only collection or for collections occurring regularly over an indefinite time period;
- explain under which of the circumstances provided for by the regulations the notice has been dispensed with; and
- advise that any concerns regarding the dispensing of notice may be brought to the attention of the Information and Privacy Commissioner.

The public statement should not disclose any personal information about an identifiable individual.

Retention of Records

The Act includes the power to make regulations relating to the retention period for personal information.

The regulations prescribe a minimum one year retention period for personal information following the last date of use of the information. The purpose of the minimum retention period is to ensure that the individual to whom the information relates has a reasonable opportunity to obtain access to the personal information [subsection 30(1)].

The one year minimum retention period can be shortened in two circumstances. First, where the individual to whom the information relates consents to an earlier disposal, the records need not be kept for one year. Individuals, however, cannot compel the destruction of records. Second, where an institution by by-law or resolution stipulates a shorter retention period for the personal information, then the shorter period becomes the minimum retention period.

This is a minimum retention period, and other operational and legal considerations may require a longer retention period.

Accuracy of Records

Subsection 30(2) requires the head of an institution to take reasonable steps to ensure that personal information is not used unless it is accurate and up to date.

Reasonable steps include checking for accuracy, including errors or omissions, at the time the personal information is collected. Any verification of information should be documented.

Although personal information may be accurate and up-to-date when collected, it may become outdated and, therefore, inaccurate. Before personal information is used, the following questions may be useful in assessing its accuracy:

- When was the information collected?
- Was the information collected directly from the individual to whom it relates?
- Was the accuracy of the information verified at the time it was collected? (e.g., Was a birth certificate viewed to verify age?)
- Is the proposed use of the information consistent with the purpose for which it was collected? Information collected for one purpose may be misleading when used for a different purpose.
- How relevant is the personal information to the current use? (e.g., If the information is used to determine eligibility for benefits based on age, the date of birth may be the most relevant piece of information.)
- What is the likelihood that the information is outdated?

Exception to Accuracy Requirement [Subsection 30(3)]

Subsection 30(2) does not apply to information collected for law enforcement purposes.

Use of Personal Information [Section 31]

This section establishes general rules governing the use of personal information in the custody and control of institutions. It recognizes that the individual's right to privacy includes the right to know how his or her personal information is being used. Personal information may be used within the institution where any one of the following circumstances exists.

Individual Consent [Subsection 31(a)]

An institution may use personal information where the individual to whom the information relates has consented to the use proposed by the institution.

This consent should be in writing and indicate:

- the particular personal information to be used;
- the use for which consent is given;

- the date of the consent; and
- the institution to which consent is given.

Consent of the individual is required where none of the other circumstances described below exists.

Purpose for Which Information Collected [Subsection 31(b)]

The institution may use personal information for the purpose for which the information was originally collected, or for a consistent purpose.

When collecting personal information, the institution must notify the subject individual of the principal purpose(s) for which the personal information is to be used. In addition, each institution is required to prepare descriptions of its personal information banks. These descriptions will list the principal uses of the personal information. The institution, therefore, may use personal information under its custody or control for the purposes indicated in the collection notice and in the personal information bank descriptions.

The institution may also use personal information for a purpose which is consistent with the purpose(s) listed in the collection notice. For an explanation of a consistent purpose, see the discussion of section 33 later in this Chapter.

For the Purpose Disclosed [Subsection 31(c)]

An institution may be in receipt of personal information disclosed to it by another institution under section 32 of this Act or by a provincial ministry or agency under section 42 of the *Freedom of Information and Protection of Privacy Act*. The receiving institution may use this personal information only for the purpose for which it was disclosed by the first institution.

For example:

> If personal information is disclosed to an institution from another institution in compassionate circumstances to assist in locating a family member [subsection 32(i)], that information is to be used by the receiving institution only to locate the family member and for no other purpose.

Disclosure of Personal Information [Section 32]

Section 32 sets out the rules for disclosure of personal information other than to the individual to whom the information relates. An institution shall not disclose personal information except in the specific circumstances enumerated in subsections 32(a) through 32(l).

Disclosure of personal information under section 32 is not dependent upon a request under the Act. Section 32 governs the disclosure of personal information in the day-to-day activities of the institution. Section 14, on the other hand, provides an exemption protecting personal privacy where a request for access has been made.

Disclosure in Accordance with Part I [Subsection 32(a)]

Subsection 32(a) permits an institution to disclose personal information in circumstances where such a disclosure would have been permitted under Part I of the Act, even though the institution had not received an access request. This subsection should be read in conjunction with subsection 50(1) which permits a head to disclose information even though an access request has not been received.

For example:

> Obligation to disclose (section 5) or compelling public interest (section 16) are

instances where the head may disclose information in the absence of a request.

Consent to Disclosure
[Subsection 32(b)]

The institution may disclose personal information where the individual has consented to the disclosure. Where this consent is not obtained in writing it should be documented and should indicate:

- the particular personal information to be disclosed;
- to whom the information may be disclosed and for what purpose it is to be used;
- the date of the consent; and the institution to which consent is given.

Consistent Purpose
[Subsection 32(c)]

The institution may disclose personal information for the purpose(s) for which it was originally collected, or for a consistent purpose. A purpose is a consistent purpose only if the individual from whom the information was directly collected might reasonably have expected such a use of the information.

For example:

A public utility commission may disclose personal information to a debt collection agency to recover monies owed to the commission for utility bills in arrears. Such disclosures would reasonably be expected by persons who have not discharged their debts to the commission.

An institution may also disclose personal information for a purpose which is consistent with the purpose(s) listed in the collection notice.

In Performance of Duties
[Subsection 32(d)]

Personal information may be disclosed to an employee or officer of the institution who needs the record in the performance of his or her duties, and where disclosure is necessary and proper in the discharge of the institution's functions. Municipal councillors are not necessarily considered officers (see County of Hastings Judicial Review).

Before an officer or employee of an institution is granted access to personal information under this provision, both of the following conditions must be satisfied:

- the employee or officer must need the record of personal information in the performance of his or her duties; and
- disclosure of the personal information must be necessary and proper in discharging the institution's functions.

Disclosures that are merely convenient or desirable would not be allowed under subsection 32(d).

An institution's functions would include the administration of by-laws, statutory programs, and activities necessary to the overall operation of the institution.

Act of Legislature or Parliament
[Subsection 32(e)]

This subsection permits an institution to disclose personal information for the purpose of complying with an act of the Legislature or of Parliament, or an agreement (i.e., collective agreement) or arrangement thereunder, or a treaty. The agreement or arrangement must result from or be sanctioned by a federal or Ontario statute. Disclosure of personal information for the purposes of complying with a regulation or a by-law would be included.

For example:

> Section 14 of the *Immunization of School Pupils Act* requires a medical officer of health to transfer a child's immunization records to another medical officer of health when that child moves to a school under the jurisdiction of the latter health unit.
>
> Subsection 72(3) of the *Child and Family Services Act* requires a person (for example, a school teacher or principal, social worker, family counsellor) to report suspicions of child abuse and to report the information on which the suspicion is based.
>
> Subsection 199(3) of the *Highway Traffic Act* requires a police officer to forward accident reports to the Ministry of Transportation.

Disclosure to Law Enforcement Agency [Subsection 32(f)]

A law enforcement institution may disclose personal information to a law enforcement agency in Canada, or to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty, or under legislative authority.

Only institutions under the *Municipal Freedom of Information and Protection of Privacy Act* which are engaged in law enforcement may disclose personal information under subsection 32(f). Law enforcement is discussed in Chapter 4.

Disclosure under subsection 32(f) may be made only to a law enforcement agency. A *law enforcement agency* includes another institution under the *Municipal Freedom of Information and Protection of Privacy Act* engaged in law enforcement, a national, state or local police agency, a municipal or provincial police agency in Canada, the RCMP, or an agency empowered by statute to enforce a law or by-law.

In exchanges of personal information with foreign countries, written agreements or treaties should be established. Where this is not possible or practical, an arrangement may be made. An *arrangement* is an unwritten agreement for the exchange of personal information.

When a law enforcement institution discloses personal information to a police agency or other law enforcement agencies in Canada, an agreement or arrangement is not required.

Aid in Law Enforcement [Subsection 32(g)]

An institution may disclose personal information to another institution covered by the *Municipal Freedom of Information and Protection of Privacy Act* or to a law enforcement agency in Canada to aid an investigation leading or likely to lead to a law enforcement proceeding.

Although this subsection permits an institution to release personal information, the institution may choose to require a search warrant before access to personal information is granted by an institution.

For example:

> The *Education Act* states that the Ontario Student Record is privileged for the information and use of supervisory officers and the principal and teachers of the school. A school may require a police agency to provide a search warrant before disclosing such a record.

Compelling Circumstances [Subsection 32(h)]

An institution may disclose personal information in compelling circumstances affecting the health or safety of an individual. In compelling circumstances, there may be no other way to obtain the personal information, or there is an emergency where the delay in obtaining the

information would be injurious to someone's health or safety. Before personal information is released under this subsection, both of the following conditions must be satisfied:

- the circumstances in which the release of personal information is contemplated must be compelling; and
- the compelling circumstances must affect the health or safety of an individual.

This section is similar to subsection 14(1)(b).

Where personal information is disclosed under this subsection, notification of the disclosure must be mailed to the last known address of the individual to whom the information relates. This means the most recent address known to the institution which disclosed the personal information. If no address is known, the institution should attempt to obtain it from the person who made the request for the information.

Compassionate Circumstances
[Subsection 32(i)]

An institution may disclose personal information in compassionate circumstances to facilitate contact with the next-of-kin, or a friend of an individual who is injured, ill or deceased.

Compassionate circumstances are those where there is a need to make contact with a friend or next-of-kin to inform them of an individual's injury, illness, or death. The personal information to be disclosed may relate either to the injured or deceased person, or to the relative or friend who is to be contacted.

Only the personal information necessary to facilitate contact should be disclosed.

Disclosure to Minister
[Subsection 32(j)]

Personal information may be disclosed to the Chairman of the Management Board of Cabinet as minister responsible for the Act.

For example:

> A request for waiver of notification of personal information under subsection 29(3)(b) may require the disclosure of personal information to the Minister.

Disclosure to Information and Privacy Commissioner
[Subsection 32(k)]

Personal information may be disclosed to the Information and Privacy Commissioner. Under subsection 41(4), the Commissioner has the authority to examine any record in the custody or control of an institution during the course of an inquiry.

Government of Canada or Government of Ontario
[Subsection 32(l)]

Disclosure of personal information is permitted to the Government of Canada or to the Government of Ontario in order to facilitate the auditing of shared-cost programs.

For example:

> Personal information contained in general welfare case files established under the *General Welfare Assistance Act* may be audited by the Province of Ontario.

Consistent Purpose
[Section 33]

Section 33 provides that when personal information is collected directly from the

individual to whom it relates, the purpose of its use/disclosure is a consistent purpose only if the individual might reasonably have expected such a use/disclosure.

Subsection 31(b) permits the use of personal information for the purpose for which it was obtained or for a consistent purpose.

Section 32(c) permits disclosure of personal information for the purpose for which it was collected or for a consistent purpose.

A consistent purpose must be compatible with the purpose stated to the individual at the time the information was collected. The individual could therefore reasonably expect this use/disclosure of his or her personal information.

For example:

> An employee of an institution could reasonably expect that personal information collected at the time of hiring might be used to assess eligibility for another position.

New Use/Disclosure of Personal Information [Subsections 35(1)(a) and (b)]

The personal information banks maintained by institutions include a statement of the regular uses of the personal information and the regular users to whom the information is disclosed.

There may be instances where the institution uses or discloses personal information for a purpose allowed by the Act, but where that use/purpose has not been listed in the personal information bank descriptions. Where such a new use or disclosure has occurred, the institution is required to:

- make a record of that new use or disclosure; and
- attach or link the record of use/disclosure to the personal information, so that when the personal information is accessed, the record of use/disclosure is accessed as well. In other words, the record of the new use/disclosure of the personal information becomes part of the personal information itself [subsection 35(2)].

If the new use or disclosure becomes a *regular* occurrence, the institution should update its personal information bank description to include the new regular use/disclosure. Once the description has been updated, section 35 ceases to apply.

The requirement to create and attach a record of use/disclosure only applies to personal information which is part of a personal information bank. It does not apply to personal information contained within a general record.

The number of these use/disclosures is included in the annual report to the Commissioner as required by section 26 of the Act.

Role of Information and Privacy Commissioner [Section 46]

Section 46 establishes the powers of the Commissioner relating to the protection of personal privacy.

Subsection 46(a) permits the Commissioner to offer comment on the privacy protection implications of proposed programs of institutions.

Subsection 46(b) enables the Commissioner to, after hearing representations from a head, order an institution to cease a collection practice and to destroy collections of personal information that contravene this Act.

Subsection 46(c) empowers the Commissioner to authorize the collection of personal information otherwise than directly from the individual to whom the information relates. (See the discussion under subsection 29(1)(c)).

Subsections 46(d), (e) and (f) respectively permit the Commissioner to engage in research into matters affecting the carrying out of the purposes of the Act, conduct public education programs about the Act and the Commissioner's role and activities and to receive representations from the public concerning the operation of this Act.

CHAPTER 6

FEES

FEES

Introduction

Some acts other than the *Municipal Freedom of Information and Protection of Privacy Act* provide that certain costs can be charged for access to records.

For example:

> Under the *Municipal Act,* the council can pass a by-law to set fees for copies of records, books and documents requested from the clerk's office. Those fees would take precedence over the fee provisions in the *Municipal Freedom of Information and Protection of Privacy Act*.
>
> Under the *Public Libraries Act a* library board can charge fees for, among other things, services other than for admission, use of library materials and reference and information services.

In the two examples above, fees can be charged for records that are available to the public without the need to make a request under the *Municipal Freedom of Information and Protection of Privacy Act*. In cases where records are not normally made available to the public for a fee and where a request is made under the Act, the person making a request may be required to pay costs incurred by the institution in processing the request [section 45].

Chargeable Costs

The costs that can be charged under the Act include personnel and other costs for searching for records and preparing them for disclosure, computer and other costs incurred by an institution, and shipping costs. These costs are specified in R.R.O. 1990, Reg. 823, section 6.

However, there are two instances where costs may not be charged. An individual is not required to pay a fee for access to his or her own personal information [subsection 45(2)]. Also, the time spent for internal decision-making concerning an access request cannot be charged to the requester.

The Goods and Services Tax (G.S.T.) is not applicable to fees charged under the Act. The costs which can be charged to the requester are outlined below.

Costs for Photocopies and Computer Printouts

An institution can charge $0.20 per page for photocopies and computer printouts. This cost includes the cost of staff time to feed documents into a photocopy machine.

An institution can charge $10.00 for floppy disks.

Search Time

A charge can be made for every hour of manual search time, in excess of two hours, that is needed to locate a record. This includes personnel time involved in searching for the records, examining file indices, file plans or listings of records, either on paper or in a computer.

After the first two hours, an institution can charge $7.50 for each 15 minutes spent by any person. If more than one person is conducting the search, each person's time can be charged.

Record Preparation Charges

Personnel time involved in physically preparing the record for disclosure can be charged.

This would include the time involved in severing exempt material prior to disclosure. Severing a record includes physical handling, for instance, putting removable tape over exempt portions of the record before it is photocopied.

An institution can charge $7.50 for each 15 minutes spent by an person for preparing a record for disclosure, including severing a part of the record.

An institution cannot charge personnel time involved in reviewing the records to determine if an exemption applies.

Computer Costs

An institution can charge $15.00 for each 15 minutes spent by any person for developing a computer program or other method of producing a record from machine readable record.

In some instances producing a record from a machine readable record will require the manipulation of information stored in a computer data base. It may be necessary to write a computer program so that the particular information requested can be retrieved.

Costs for Services Outside the Institution

Computer and other costs incurred in locating, retrieving, processing and copying a record can be charged to the requester if those costs are specified in an invoice received by the institution.

An institution may require outside services to assist in locating, retrieving, processing or copying records. Where an institution receives an invoice for the cost of outside services, the costs can be passed on to the requester.

For example:

> A request might be for a copy of a record in a format other than a photocopy, computer printout or a computer disc. If an institution does not have the capabilities to do specialized copies, such as microfilm or fiche, the institution can send the material to outside facilities for copying.

However, before using outside services the institution should ensure that the cost for using outside services would not be greater than the cost of handling the matter internally.

Shipping Costs

Shipping charges such as postage or courier costs can be charged.

Fee Estimates and Deposits

Where a fee estimate is $25.00 or more, the institution may require the requester to pay a deposit equal to 50% of the estimate before completing the request.

For example:

> If the estimated cost for processing a request is $40.00, a deposit of $20.00 may be required. If, after processing, it is determined that the actual fee is $45.00, the requester would be billed $25.00 as the balance of the fee.

An institution is not required to release records to a requester until the fee has been paid, or the issue of fees has been resolved after an appeal to the Office of the Information & Privacy Commissioner.

See Chapter 3 for the procedure for calculating fee estimates.

Waiving Fees

A head shall waive all or part of the fees if in the head's opinion it is fair and equitable to do so after considering:

- the extent to which the actual cost of processing, collecting and copying the record varies from the amount of payment required by the section;

- whether the payment will cause a financial hardship to the person requesting the record;
- whether dissemination of the record will benefit public health or safety;
- whether the person requesting access to the record is given access to it; and
- if the amount of a payment would be $5.00 or less, whether the amount of the payment is too small to justify requiring payment.

A head's decision not to waive a fee may be appealed to the Information and Privacy Commissioner [subsection 45(5)].

CHAPTER 7

COMMISSIONER AND APPEALS

COMMISSIONER AND APPEALS

Introduction

The *Municipal Freedom of Information and Protection of Privacy Act* gives persons a right to appeal decisions about access to records that are made by institutions covered by the Act. Appeals are filed with the Information and Privacy Commissioner (hereafter referred to as the Commissioner) who is an officer of the Ontario Legislature and is independent of the government or any institution.

This chapter outlines the powers of the Commissioner and the appeal process. Many of the procedures have been developed by the Information and Privacy Commission and are subject to change. Where clarification is needed during an appeal, the institutions should contact the Appeals Officer assigned to the appeal.

Information and Privacy Commissioner

The Appointment of the Commissioner

The Commissioner is appointed by the Lieutenant Governor in Council. The Commissioner is an officer of the legislature and is independent of the government.

The Commissioner is appointed for a term of five years and may be reappointed for a further term or terms. The Commissioner is removable at any time for cause by the Lieutenant Governor in Council on the address of the Assembly.

The Powers of the Commissioner on Appeal

The Commissioner makes decisions in respect of appeals by issuing an order [subsection 43(1)]. The order may contain any conditions the Commissioner considers appropriate [subsection 43(3)]. Orders made by the Commissioner are binding on all parties to the appeal. It is an offence to wilfully fail to comply with an order of the Commissioner [subsection 48(1)(f)].

Once the order is made, the Commissioner must give notice of the order to the appellant, the institution and any other affected person [subsection 43(4)].

Where the head has exercised his or her discretion to rely on a discretionary exemption to withhold a record, the Commissioner shall not order the head to disclose the record or part of it. However, the Commissioner may order the head to consider the exercise of discretion, where the head has not done so.

If the Commissioner determines that the record or part does not fall within an exemption, the Commissioner will order that the record be disclosed.

What Can Be Appealed?

An appeal is to be made within 30 calendar days after the notice is given of the decision appealed [subsection 39(2)]. However, where the institution cannot show that it is prejudiced by the delay, appeals launched after the 30-day time period may be allowed.

For example:

> Prejudice may be established where the records referable to the appeal have been destroyed.

Generally, any decision that a head makes under the Act may be appealed to the Commissioner. The decisions that can be appealed include:

- a decision to extend the time limit for responding to a request under section 20;
- refusal to grant access to a record on the ground that the record does not exist;

- refusal to grant access to a record on the ground that the record is exempt;
- granting access to only part of the record;
- granting a request for access to a record or part that may contain information referred to in section 10 (third party information) or that contains personal information where the disclosure may be an unjustified invasion of personal privacy under subsection 14(1)(f);
- refusal to confirm or deny the existence of a record that deals with law enforcement [subsection 8(3)] or would, if disclosed, be an unjustified invasion of personal privacy [subsection 14(5)];
- a deemed refusal to grant access to records under subsection 22(4);
- a refusal to make a correction to personal information requested under subsection 36(2)(a);
- the amount of a fee charged under section 45;
- refusal to waive a fee charged under section 45; and
- refusal to allow a requester to examine the original record under sections 23 or 37.

Who Can Appeal?

The following persons can appeal to the Commissioner:

- a person who has made a request for access to a record under subsection 17(1);
- a person who has made a request for access to his or her own personal information under subsection 37(1);
- a person who has requested correction of his or her own personal information under subsection 36(2); and
- an affected third party who has received a notice under subsection 21(1) that the head intends to disclose a record that may affect the interests of the third party.

The Appeal Process

Notice of Appeal by Requester

An appeal is initiated by the requester by filing a written notice of appeal with the Commissioner. Many times the notices are vague and lacking in details that would enable the Commissioner to understand what is being appealed. It is recommended that decision letters sent by institutions include a paragraph informing the requester that he or she can appeal the decision to the Commissioner's Office within 30 days. Let the requester know that an appeal should be accompanied by:

- the file number assigned to the request by the institution;
- a copy of the decision letter; and
- a copy of the original request for information.

Upon receiving a notice of appeal, the Commissioner must notify the head of the institution that an appeal of the head's decision has been filed. The Commissioner must also notify any other person who, in the Commissioner's opinion, is "affected" by the appeal [subsection 39(3)]. The institution's Freedom of Information and Privacy Coordinator should also be notified.

Where the head has any information concerning the affected persons who should be notified of the appeal, this information should be conveyed to the Appeals Officer assigned to the case. The

affected persons should contact the Freedom of Information and Privacy Coordinator for further information about the appeal.

Confirmation of Appeal

The Commissioner's Office notifies an institution that an appeal has been filed by sending out a "Confirmation of Appeal" letter. It generally advises the institution the name of the requester, the Commissioner's appeal number and the name of the Appeals Officer assigned to the case.

The "Confirmation of Appeal" letter also asks the institution to provide the following information where applicable:

- a copy of the original request;
- the notice of the head's decision;
- any correspondence related to the request or decision making process;
- an index of records and exemptions; and
- the record (severed and unsevered copies).

Where the appeal relates to either a time extension or a fee matter, the request for the last two items on the list will be omitted. Additional information may also be forthcoming at this time that will assist the institution to deal with the appeal promptly and efficiently.

Duty to Provide Records

The "Confirmation of Appeal" letter assumes that the institution's Freedom of Information and Privacy Coordinator will provide the records relevant to the appeal to the Appeals Officer. The Commissioner's Office requires that these records be produced within two weeks of the date of confirmation notice.

Where an institution fails to provide the records within the two-week period, the Commissioner can issue an order for the production of records. Failure to provide the records to the Commissioner may result in a prosecution for wilful obstruction [subsection 48(1)(d)].

The Commissioner may call for and examine any record that is in the custody and under the control of an institution, despite Parts I and II of this Act or any other Act or privilege [subsection 41(4)]. Subsection 41(12) states that where records are provided no one is liable to prosecution for an offence against any other Act because of the provision of records. The Commissioner may not delegate his or her authority to any person other than an Assistant Commissioner, the power to require a record referred to in section 8 (law enforcement) to be produced and examined [section 44].

While the Commissioner may require records to be produced, and may enter and inspect any premises occupied by an institution for the purposes of the investigation [subsection 41(4)], the head, in exceptional circumstances, may require that the examination of a record by the Commissioner be of the original at its site [subsection 41(6)]. This power of the head may be invoked, for example, if the record is fragile, unique or involves a large volume of records.

Before entering any premises, the Commissioner must notify the head of the institution occupying the premises of his or her purpose [subsection 41(7)].

Mediation

According to section 40 of the Act, the Commissioner may authorize a mediator to investigate the circumstances of any appeal and to try to effect a settlement of the matter under appeal.

An Appeals Officer assigned to an appeal will review the circumstances of the case and verify the institution's position. Acting as a go-between, he or she will also try to settle the appeal or simplify the issues, based on discussions with the appellant and the institution [section 40]. In a mediated settlement both parties reach an agreement about the matter under appeal.

The Office of the Information and Privacy Commissioner will attempt to settle the issues at appeal before resorting to an order. The general time period allotted for mediation is three months. This time period may be shortened if it is apparent that no agreement can be reached. The appeal will then proceed to an inquiry.

The Inquiry

Where mediation is unsuccessful, the Commissioner is required to conduct an inquiry to review the head's decision [subsection 41(1)]. At this stage, the appellant and the institution receive a "Notice of Inquiry" letter. This notice advises the parties to an appeal that they are entitled to make representations, usually in writing, to the Office of the Information and Privacy Commissioner.

Generally the Notice of Inquiry will supply the parties to the appeal with concise background information and will summarize the facts and issues in the appeal. The Notice of Inquiry will also focus on identifying the requirements of exemption claims as they arise in particular appeals.

The Notice of Inquiry will contain specific questions that relate directly to the issue at appeal. These questions are to be answered by the institution and any other party to the appeal. The representations need not be limited to the questions posed in the Notice of Inquiry. Parties may submit additional facts which bear on the appeal.

Burden of Proof

According to section 42, where a head of an institution denies access to a record or part of a record, the institution must prove on appeal that the record, or part, falls within an exemption under the Act. If an affected third party does not want the record or part to be released, the third party has to prove that the record or part should be exempt from disclosure.

The onus of proving the application of an exemption or an exception to an exemption is on the party claiming the exemption.

Written or Oral Representations

Inquiries in respect of access to records must be conducted in a manner which protects the confidentiality of records. Therefore, the normal rules governing the rights of parties appearing before tribunals do not apply [subsection 41(2)]. These include the right to a public hearing and the right to cross-examine witnesses.

An inquiry may be conducted in private [subsection 41(3)]. The Commissioner's normal practice is to conduct inquiries through written representations, however an appellant or institution may request an opportunity to make oral submissions.

For example:

> Where an appellant cannot, by reason of disability, provide written submissions, an oral hearing may be held.

The Commissioner has the power to summon and examine on oath any person who may have information relating to the inquiry [subsection 41(8)]. Anything said or any document produced during an inquiry is privileged in the same manner as if the inquiry were a proceeding in a court [subsection 41(9), (10) and (11)]. Testimony provided during an inquiry may not be used in other proceedings, except in

respect of a prosecution for perjury [subsection 41(10)].

All parties to the appeal must be given the opportunity to make representations, however, no person is entitled to be present during, to have access to or to comment on representations made to the Commissioner by any other person [subsection 41(13)]. The institution, the appellant and any affected party may be represented by counsel or an agent [subsection 41(14)].

Compliance Investigations

The *Municipal Freedom of Information and Protection of Privacy Act* recognizes that institutions should have basic standards for protecting personal information in its possession. The privacy provisions of the Act require institutions to use appropriate practices and procedures for collecting, storing, using, disclosing and ultimately disposing of personal information.

The Compliance Department of the Commissioner's office initiates an investigation when a public complaint is received; when an appeal raises compliance or privacy issues; or when the Commissioner's office determines that a particular issue warrants investigation. Compliance Investigators are directed to conduct a thorough review of an institution's practices and procedures and to report findings to the Assistant Commissioner (Privacy).

Judicial Review

The Commissioner has the power to issue a binding order which is not subject to an appeal. Appeals are distinct from judicial review proceedings. Judicial review proceedings are governed by the *Judicial Review Procedure Act*. Applications for judicial review may be brought before Divisional Court by a party to an appeal where it is alleged that the Commissioner has made a serious error or where substantial wrong or miscarriage of justice has occurred.

In the order issued by the Commissioner, the party against whom the order is made is advised of the right to apply for judicial review and given 30 days to make the application. Where no application for judicial review is made within that period, the party must comply with the order.

CHAPTER 8

OFFENCES AND LIABILITY

OFFENCES AND LIABILITY

Offences [Section 48]

Section 48 of the Act outlines offences under the *Municipal Freedom of Information and Protection of Privacy Act*, the penalty for offences and when the consent of the Attorney General is required for prosecutions.

Subsections 48(1)(a), (b) and (c) create offences relating to breaches of the privacy protection provisions of the Act.

Subsections 48(1)(d), (e) and (f) create offences relating to the obstruction of the Information and Privacy Commissioner in the carrying out of his or her duties or exercising his or her powers.

It is an offence to wilfully disclose personal information in contravention of the Act [subsection 48(1)(a)]. The offence consists of intentionally and knowingly disclosing personal information in a manner that is not authorized by the Act.

It is an offence to wilfully maintain a personal information bank that contravenes the Act [subsection 48(1)(b)]. The offence in this case is to intentionally maintain a secret personal information bank that is not described and made public as required by section 34. The Information and Privacy Commissioner may order the destruction of a collection of personal information that contravenes the Act. The Commissioner may also order an institution to cease collecting certain types of personal information.

It is an offence to make a request under this Act for access to or correction of personal information under false pretences [subsection 48(1)(c)].

Subsections 48(1)(d), (e) and (f) create offences relating to the obstruction of the Information and Privacy Commissioner in the carrying out of his or her duties or exercising his or her powers.

It is an offence to wilfully obstruct the Commissioner in the performance of his or her functions under the Act [subsection 48(1)(d)]. Subsection 48(1)(e) creates an offence of wilfully making a false statement to mislead or attempt to mislead the Commissioner. It is an offence to wilfully fail to comply with an order of the Commissioner [subsection 48(1)(f)].

A person who is found guilty of an offence is liable to a fine not exceeding $5,000 [subsection 48(3)].

A prosecution cannot be commenced under subsections 48(1)(d), (e) or (f) without the consent of the Attorney General.

Liability [Subsections 49(2) and (3)]

Civil actions cannot be brought against an employee of an institution for monetary damages resulting from the disclosure or non-disclosure of a record under the Act, if the action was done in good faith. Subsection 49(2) also provides that no civil action can be brought against an employee for failure to give a required notice under the Act if reasonable care was taken to give notice.

The Act preserves the liability of institutions, as opposed to the individual employee, to civil proceedings for damages, however an employee's actions can make an institution liable.

APPENDICES

APPENDIX I

SAMPLE BY-LAW

THE CORPORATION OF THE
[insert name]
BY-LAW NO. 92-00

Being a By-law to designate a head of the Municipal Corporation for the purposes of the *Municipal Freedom of Information and Protection of Privacy Act*.

Whereas, under Section 3, subsection 1 of the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c.M.56, the council of a municipal corporation may by by-law designate from among its members an individual or a committee of the council to act as head of the municipal corporation for the purposes of the Act:

And, whereas the council deems it necessary and expedient to designate a head for the purposes of the Act:

NOW THEREFORE THE COUNCIL OF THE CORPORATION OF THE [INSERT NAME] ENACTS AS FOLLOWS:

1. That [**name/position of member of council or committee of council**] be designated as head for the purposes of the *Municipal Freedom of Information and Protection of Privacy Act*.

2. That this by-law come into force and effect on [insert date here].

Read a first and second time this _____ day of _____, 19____.

_____ _____
[Clerk] [head of Council]

Read a third time and passed this _____ day of _____, 19____.

_____ _____
[Clerk] [head of council]

[seal of the municipal corporation]

APPENDIX II

SAMPLE RESOLUTION

RESOLUTION
FOR A BOARD, COMMISSION OR OTHER BODY

MOVED BY:

SECONDED BY:

Whereas, under Section 3, subsection (2) of the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990 c.M.56 the members elected or appointed to a board, commission or other body that is an institution under the Act may designate in writing from among its members an individual or committee of the body to act as head of the institution for the purposes of the Act:

And whereas the **[board, commission or other body]** deems it necessary and expedient to designate a head for the purposes of the Act:

Now, therefore, the **[board, commission or other body]** resolves as follows:

1. That the **[board, commission or other body]** hereby designates **[name/position of individual or committee]** as head for the purposes of the *Municipal Freedom of Information and Protection of Privacy Act*.

2. That this resolution come into force and effect on [insert date here].

_____ _____

[SECRETARY] [CHAIRPERSON]

APPENDIX III

SAMPLE DELEGATIONS OF AUTHORITY

Sample 1

I/we, **[head of the institution for the purposes of the Act]**, delegate the following powers and duties under the Municipal Freedom of Information and Protection of Privacy Act to the positions indicated below:

Power or Duty **Officer:**	**A**	**B**	**C**
Severing records (s.4(2))	X		
Obligation to disclose (s.5)		X	
Deciding if exemptions apply:			
• draft by-laws, private bills, closed meetings (s.6)		X	
• advice or recommendations (s.7)		X	
• law enforcement (s.8)		X	
• relations with governments (s.9)		X	
• third party information (s.10)		X	
• economic and other interests (s.11)		X	
• solicitor-client privilege (s.12)		X	
• danger to safety or health (s.13)		X	
• personal privacy (s.14)		X	
• information available or soon to be published (s.15)		X	
• individual's access to own personal information (s.38)		X	
Determining compelling public interest (s.16)		X	
Assisting requester clarify requests (s.17(2))	X		
Forwarding and transferring requests (s.18)	X		
Issuing Notices:			
• forwarding or transferring requests (s.18(2),(3))	X		

	A	B	C
• regarding access to records (s.19, 21, 22)	X		
• time extensions (s.20)	X		
• to affected parties (s.21)	X		
Decisions *re* manner of third party representations (s.21(6))		X	
Granting access to original record (s.23)	X		
Making record descriptions available (s.25, 34)	X		
Preparing annual report (s.26)	X		
Notice of collection of personal information (s.29(2))	X		
Ensuring accuracy of personal information (30(2))	X		
Disposal of personal information (s.30(4))	X		
Personal information banks (s.35)	X		
Access to personal information (s.37(3))	X		
Representing institution on appeal (s.41)			X
Requiring examination of record on site (s.41(6))	X		
Fees (s.45)	X	X	
Providing access - oral requests (s.50)			

Date _____ Signature(s) _____

Sample 2

I/we **[head of the institution for the purposes of the Act]**, delegate all powers and duties under the Municipal Freedom of Information and Protection of Privacy Act to **[position title]**.

Date _____ Signature(s) _____

APPENDIX IV

SAMPLE NOTIFICATION LETTERS

- Notice of receipt of request
- Clarifying requests
- Forwarding or transferring requests
- Notice of time extension
- Fee estimate/interim notice decision regarding disclosure
- Notice to affected third party (section 10: third party information)
- Notice to affected third party (section 14: personal privacy)
- Notice to requester where third party is affected
- Notice to affected third party after representations where head intends to release the record(s)
- Notice to requester granting access to records
- Notice to requester denying access to records or parts of records
- Notice to requester *re* response to a correction request

See Chapter 3 (Access Procedures) for a detailed discussion of when notifications are required during the processing of a request.

Notice of Receipt of Request

[Date]

[Requester's name and address]

Dear _____:

Your request for access to **[insert details of records requested]** was received on **[insert date]** by **[insert name of institution]**. We will respond to your request according to the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*.

Please contact **[name, title and phone number of person responsible]** if you have any further questions.

Sincerely,

[signed by head or delegate]

Clarifying Requests

[Date]

[Requester's name and address]

Dear _____:

Your request for access to records under the *Municipal Freedom of Information and Protection of Privacy Act* was received on **[insert date]**.

Unfortunately, the request does not provide sufficient detail to enable us to identify the record(s). Please supply us with the following information that will help us identify the record(s) you have requested:

[insert details]

Please contact **[name, title and phone number of person responsible]** if you have any further questions.

Sincerely,

[signed by head or delegate]

Forwarding or Transferring Requests

[Date]

[Requester's name and address]

Dear _____:

Your request under the *Municipal Freedom of Information and Protection of Privacy Act* for access to **[describe record(s) requested]** was received on **[insert date]**.

Section 18 of the Act states that an institution that receives a request for a record and does not have it in its custody or under its control, shall forward the request to another institution if the head decides that the other institution has custody or control of the record. Your request has been forwarded to **[name and address of head of other institution]**. That institution has custody or control of the record(s) you have requested.

[OR]

Section 18 of the Act states that if an institution receives a request for a record and it considers that another institution has a greater interest in the record, the head may transfer the request to the other institution. Your request has been transferred to **[name and address of head of other institution]**. That institution has a greater interest in the records you have requested.

You may appeal this decision to the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

Please note that you have 30 days from the receipt of this letter to request a review.

Please contact **[name, title and phone number of head or delegate at second institution]** if you have any further questions.

Sincerely,

[signed by head or delegate]

NOTE: **As quickly as possible, the head or delegate should notify the other institution that a request is being forwarded/transferred**

Notice of Time Extension

[Date]

[Requester's name and address]

Dear _____:

Your request under the *Municipal Freedom of Information and Protection of Privacy Act* for access to **[describe records requested]** was received on **[insert date]**.

Under the Act the general time limit for responding to access requests is 30 days. We wish to advise you that the time limit for responding to your request has been extended in accordance with section 20 of the Act. The time will be extended for an additional **[insert number]** days to **[insert date]**.

The reason for the time extension is **[insert reason]**:

You may request that our decision to extend the time limit be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

Enclosed is a copy of section 20 of the Act for your convenience and information **[optional]**. Please contact **[name, title and phone number of person responsible]** if you have any further questions.

Sincerely,

[signed by head or delegate]

Fee Estimate/Interim Decision Regarding Disclosure

[Date]

[Requester's name and address]

Dear _____:

Further to your request for access to records under the *Municipal Freedom of Information and Protection of Privacy Act*, it is expected that the fees we are permitted to charge under section 45 will apply to your request. The estimated fee is **[enter amount]**. The fee estimate is based on **[explain fee estimate]**.

Our preliminary review of the records indicates that some of the following exemptions might apply to the records you have requested. **[Generally describe what exemptions might apply to the records]**.

The Act provides that all or part of the fee can be waived if in our opinion it is fair and equitable to do so, if the fee will cause you financial hardship or if dissemination of the record will benefit public health or safety. You may be required to provide proof to support any waiver claims. Please notify **[insert name, title and phone number]** as soon as possible of your wish to proceed with a request for a fee waiver.

Your written acceptance of this fee estimate is requested prior to proceeding with the request.

[OR: Where the fee estimate is over $25.00]

Pursuant to Ontario Regulation 517/90, where the fee estimate is over $25.00, an institution is permitted to request a deposit equal to 50% of the estimated fee. If you wish to proceed with the request it will be necessary for you to submit a cheque in the amount of **[enter amount]** prior to proceeding with the request.

If you disagree with any aspect of the fees, please discuss it with us. Afterward, you may request that this fee estimate be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

Please note that you have 30 days from the receipt of this letter to request a review.

Enclosed is a copy of section 45 of the Act for your convenience and information **[optional]**. Please contact **[name, title and phone number of person responsible]** with any questions.

Sincerely,

[signed by head or delegate]

Notice to Affected Third Party - Section 10: Third Party Information

[Date]

[Affected third party's name and address]

Dear _____:

The [**name of institution**] has received a request for access to records under the *Municipal Freedom of Information and Protection of Privacy Act* to disclose [**describe in detail the records as they relate to the affected third party**].

According to section 21 of the Act, a third party whose interests may be affected must be given the opportunity to make representations to the head of an institution concerning disclosure of the records.

To successfully qualify for a third party exemption, *all* of the following three tests must be met:

- the information must fit within one of the specified categories of third party information; trade secret or scientific, technical, commercial, financial or labour relations information;
- the information must have been *supplied* by the third party *in confidence,* implicitly or explicitly; and
- the disclosure of the information could reasonably be expected to cause one of the harms indicated below:
    - prejudice your competitive position or interfere with any contractual rights you possess, or
    - result in you no longer supplying this or similar information to [**name of institution**], or
    - result in undue loss or gain to any person, business, or organization of which you are aware.

Under section 10 of the Act, we are obliged to release these records unless the above conditions are met.

Notice to Affected Third Party - Section 10: Third Party Information, (Continued)

Your opinions regarding the disclosure of these records would be appreciated. If you have concerns about the release of the records please contact us, in writing, no later than [insert date] outlining your concerns. In order to support your claims against the release of the documents, you must provide us with factors that speak to section 10 of the Act. Speculation will not be considered a cogent argument.

You will be notified in writing by **[insert date]** about our decision regarding the release of the records.

Enclosed are copies of sections 10 and 21 of the Act for your convenience and information **[optional]**. Please contact **[name, title and phone number of person responsible]** if you have any further questions.

Sincerely,

[signed by head or delegate]

Notice to Affected Third Party - Section 14: Personal Information

[Date]

[Affected third party's name and address]

Dear _____:

The [**name of institution**] has received a request under the *Municipal Freedom of Information and Protection of Privacy Act* to disclose [**describe in detail the records as they relate to the affected individual**].

Pursuant to section 21 of the Act, we must give an individual the opportunity to make representations about the release of the records.

Your opinions regarding the disclosure of these records would be appreciated. Please indicate in writing whether or not you consider that the disclosure of these records would be an invasion of your personal privacy. Section 14 of the Act outlines circumstances where the disclosure of personal information may be an unjustified invasion of personal privacy.

Your response must be received no later than [**insert date**]. You will be notified in writing by [**insert date**] about our decision regarding the release of the records.

Enclosed are copies of sections 14 and 21 of the Act for your convenience and information [**optional**]. Please contact [**name, title and phone number of person responsible**] if you have any further questions.

Sincerely,

[signed by head or delegate]

Notice to Requester Where Third Party is Affected

[Date]

[Requester's name and address]

Dear _____:

Your request for access to records under the *Municipal Freedom of Information and Protection of Privacy Act* was received on **[insert date]**. The disclosure of the records may affect the interests of a third party.

A third party whose interests may be affected is being given the opportunity to make representations about the release of the records.

A decision on whether or not the record will be disclosed will be made by **[insert date]**, in accordance with section 21 of the Act.

Enclosed is a copy of section 21 of the Act for your convenience and information **[optional]**. Please contact **[name, title and phone number of person responsible]** if you have any further questions.

Sincerely,

[signed by head or delegate]

Notice to Affected Third Party After Representations Where Head Intends to Release the Record(s)

[Date]

[Affected third party's name and address]

Dear _____:

We have received your representations concerning disclosure of [**details of the record(s)**]. We have considered your representations, however a decision has been made to grant access [**or partial access**] to the record(s). [**Give reasons for the decision**].

In accordance with section 21 of the *Municipal Freedom of Information and Protection of Privacy Act*, you may request that this decision be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

You have until [**insert date**] to request a review, otherwise the records will be released to the requester.

Please contact [**name, title and phone number of person responsible**] if you have any further questions.

Sincerely,

[signed by head or delegate]

Notice to Requester Granting Access to Records

[Date]

[Requester's name and address]

Dear _____:

I am responding to your request under the *Municipal Freedom of Information and Protection of Privacy Act* for access to **[describe records requested]**.

Access is granted to the records you have requested.

Sincerely,

[signed by head or designate]

NOTE: **In this notice, the institution may wish to:**

- **indicate the fees for access to the records, if any;**
- **give the requester the option to view the record; or**
- **indicate that identification will be required if access is given to an individual's own personal information**

Notice to Requester Denying Access to Records or Parts of Records

[Date]

[Requester's name and address]

Dear _____:

I am responding to your request under the *Municipal Freedom of Information and Protection of Privacy Act* for access to **[describe records requested]**.

Unfortunately, we must deny access to **[insert details of withheld records]** pursuant to section(s) **[insert section numbers]** of the Act. The provisions apply to the record(s) because **[insert reasons]**.

You may request that this decision be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

Please note that you have 30 days from the receipt of this letter to request a review.

Enclosed is a copy of section **[insert relevant section number]** of the Act for your convenience and information **[optional]**. Please contact **[name, title and phone number of person responsible]** if you have any further questions.

Sincerely,

[signed by head or designate]

NOTE: **In this notice (if partial access is granted), the institution may wish to:**

- **indicate the fees for access to the records, if any;**
- **give the requester the option to view the record; or**
- **indicate that identification will be required if access is given to an individual's own personal information**

Notice to Requester - Correction of Personal Information

[Date]

[Requester's name and address]

Dear _____:

Your request under the *Municipal Freedom of Information and Protection of Privacy Act* for a correction of personal information was received on **[insert date]**.

The correction was made and a copy of the corrected record is attached. On request, you are entitled to have the correction sent to those persons to whom the information was disclosed over the past 12 months.

OR

The correction was not made to the personal information. You are entitled to require that a statement of disagreement be attached to the record and that the statement of disagreement be sent to any person to whom the record was disclosed over the past 12 months.

You may appeal this decision to the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

Please note that you have 30 days from the receipt of this letter to request a review.

Sincerely,

[signed by head or designate]

NOTE: **With this notice, the institution may wish to:**

- **include a listing of the persons to whom the personal information was disclosed over the past 12 months (this listing will not include those persons listed in the personal information bank index)**

Notice to Requester - Correction of Personal Information

[Date]

[Requester's name and address]

Dear _____:

Your request under the *Municipal Freedom of Information and Protection of Privacy Act* for a correction of personal information was received on **[insert date]**.

The correction was made and a copy of the corrected record is attached. On request, you are entitled to have the correction sent to those persons to whom the information was disclosed over the past 12 months.

OR

The correction was not made to the personal information. You are entitled to require that a statement of disagreement be attached to the record and that the statement of disagreement be sent to any person to whom the record was disclosed over the past 12 months.

You may appeal this decision to the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

Please note that you have 30 days from the receipt of this letter to request a review.

Sincerely,

[signed by head or designate]

NOTE: With this notice, the institution may wish to:

- **include a listing of the persons to whom the personal information was disclosed over the past 12 months (this listing will not include those persons listed in the personal information bank index)**

APPENDIX V

A CHECKLIST FOR THE RECRUITMENT AND HIRING PROCESS

The following is a brief discussion of the impacts which the privacy protection provisions of Part II of the *Municipal Freedom of Information and Protection of Privacy Act* has on the recruitment and hiring process. These matters are discussed in more detail in Chapter 5 of this handbook.

Collecting Personal Information During Recruitment

The three main provisions of Part II of the Act affecting the collection of information about job applicants are:

- the authority to collect personal information [subsection 28(2)];
- the authority to collect personal information indirectly [subsection 29(1)]; and
- the notification requirements when personal information is collected [subsection 29(2)].

The "Application for Employment" Form

An application for employment form collects personal information on job applicants directly from the individual. Subsection 29(2) of the Act requires that a notice of collection be given to the job applicant. The notice would usually be placed on the application form itself.

This notice must contain:

- a statement about the legal authority for the collection. Usually, this will be the legislation which establishes the institution (e.g., the *Municipal Act* for municipalities, the *Education Act* for school boards), or a by-law or resolution which authorizes a particular competition;
- a statement of the purpose of the collection; and
- the title, business address and phone number of an employee who can answer questions about the collection of the personal information.

A notice on an application form might read:

> Personal information on this form is collected under the authority of [**name of statute; or by-law no.; or resolution no.**], and will be used to determine eligibility for employment. Questions about this collection of personal information should be directed to [**title, business address and phone number of appropriate employee (e.g., Human Resources Manager)**].

Receiving Resumes From Applicants

Where resumes (as opposed to application forms) are received as a result of an advertised job posting, the notice of collection of personal information is still required.

The notice must contain the same information as discussed above in relation to application forms. This notice could be incorporated into a standard acknowledgement letter, or could form part of the advertised job posting.

Unsolicited applications and resumes submitted by individuals on their own initiative, and which are not retained or used by the institution are not *collected* by the institution. Accordingly, notice of collection under subsection 29(2) need not be provided to the individual.

Where an unsolicited resume is retained in an inventory or is entered into a specific job competition, notice of collection of personal information is required unless a waiver has been obtained from the Information and Privacy Commissioner.

Collecting Information During an Interview

The rules relating to the authority to collect personal information and the requirement to provide a notice of collection also apply to *non-recorded* information [subsection 28(1)]. The collection of personal information must be:

- authorized by statute;
- used for law enforcement purposes; or
- necessary for the administration of a lawfully authorized activity.

Only that personal information which is relevant to and necessary for the lawfully authorized activity should be collected during the interview. Institutions must ensure that information is collected in accordance with the Ontario Human Rights Code. Questions relating to age, marital status, ethnic origin, etc., may not be asked during an interview. However, where institutions are required to meet specific employment equity quotas, questions may be asked to determine if an individual falls into one of the following categories; aboriginal peoples, persons with disabilities, visible minorities or women.

There is no requirement in the Act that a record be made of verbally collected information. However, it is a good practice to make such a record to document decisions.

Checking References

Collecting personal information about an applicant from a reference source is an indirect

collection under subsection 29(1) of the Act. The consent of the applicant is required for the institution to contact references.

A consent form containing the following information could be used at any stage in the recruitment process:

I, **[name of individual]** authorize **[name of institution]** to contact the person or organization listed below for the purpose of obtaining reference information including information contained in my personnel file. These persons are authorized to disclose such information:

[insert name, position title and phone number of persons to contact]

Date: _____ Signed: _____

Giving References

Before a staff member of the institution discloses personal information in a reference (i.e., where you are being asked to provide a reference), he or she must have the consent of the individual. Subsection 32(a) allows disclosure of personal information with the consent of the individual.

APPENDIX VI

Sample Biography

SAMPLE BIO:
JANE CITIZEN

Jane Citizen, of Anyplace, Ont. was recently appointed to the Anyplace Advisory Committee for Parks and Recreation.

Ms. Citizen has lived in Anyplace for the past 10 years. She has considerable volunteer experience in the community, having served as a board member for several local recreational associations, as the president of the Anyplace Tennis Club, and as president of the West Anyplace Neighbourhood Association. She is also a former medal winner for Canada in speed skating at the 1968 Olympics.

Ms. Citizen is President of Jane Citizen Electronics in Anyplace. She has a degree in engineering from the University of Toronto.

INDICES

INDICES

Section Index

Sections without page references are not specifically addressed in the text.

Subject Index

D

E

F

G

O

P

R

S

T

U

V

W

Y

ACCO®

ACCOPRESS™

YELLOW	25070	JAUNE
*BLACK	25071	NOIR*
*BLUE	25072	BLEU*
RL. BLUE	25073	RL. BLEU
*GREY	25074	GRIS*
GREEN	25075	VERT
RUST	25078	ROUILLE
EX RED	25079	ROUGE

ACCO CANADA INC.
WILLOWDALE, ONTARIO

* INDICATES 75% RECYCLED 25% POST-CONSUMER FIBRE

*SIGNIFIE 75 % FIBRES RECYCLÉES, 25 % DÉCHETS DE CONSOMMATION

BALANCE OF PRODUCTS 25% RECYCLED

AUTRES PRODUITS: 25 % FIBRES RECYCLÉES